

METHOD AND SYSTEM FOR BIOMETRIC RECOGNITION  
BASED ON ELECTRIC AND/OR MAGNETIC CHARACTERISTICS



CROSS-REFERENCE

U.S. patent application 08/974,281 filed November 20,  
5 1997, by Juliana H. J. Brooks titled "Method and System for  
Biometric Recognition Using Unique Internal Distinguishing  
Characteristics", incorporated by reference herein.

U.S. provisional patent application 60/099,995 filed on  
September 11, 1998, titled "Detection, Identification, Augmentation  
10 and/or Disruption of Inorganic, Organic, or Biological Structures  
Using Resonant Acoustic and/or Acoustic-EM Energy", having Attorney  
Docket No. BLB:106PRV, incorporated by reference herein.

U.S. patent application 09/151,581 filed September 11,  
1998, by Juliana H. J. Brooks titled "Generation and Detection of  
15 Induced Current Using Acoustic Energy".

U.S. patent application 09/151,332 filed September 11,  
1998, by Juliana H. J. Brooks titled "Measurement of Electric  
and/or Magnetic Properties in Organisms Using Induced Currents".

U.S. patent application 09/151,897 filed September 11,  
20 1998, by Juliana H. J. Brooks titled "Measurement of Electric  
and/or Magnetic Properties in Organisms Using Electromagnetic  
Radiation".

U.S. patent application 09/151,908 filed September 11, 1998, by Juliana H. J. Brooks titled "Method and System for Biometric Recognition Based on Electric and/or Magnetic Properties".

5 U.S. patent application 09/151,847 filed September 11, 1998, by Juliana H. J. Brooks titled "Method and System for Biometric Recognition Using Sensors with Unique Characteristics".

#### FIELD OF THE INVENTION

10 The present invention relates generally to the detection of electric and/or magnetic properties in an individual living organism. More specifically, the present invention relates to biometric recognition wherein electric and/or magnetic properties of an organism are used to recognize the organism.

#### BACKGROUND OF INVENTION

15 Security methods based on memory data encoded into magnetic cards such as personal identification numbers or passwords are widely used in today's business, industrial, and governmental communities. With the increase in electronic transactions and  
20 verification there has also been an increase in lost or stolen cards, and forgotten, shared, or observed identification numbers or passwords. Because the magnetic cards offer little security against fraud or theft there has been a movement towards developing

more secure methods of automated recognition based on unique, externally detectable, personal physical anatomic characteristics such as fingerprints, iris pigment pattern and retina prints, or external behavior characteristics; for example, writing style and voice patterns. Known as biometrics, such techniques are effective in increasing the reliability of recognition systems by identifying a person by characteristics that are unique to that individual. Some representative techniques include fingerprint recognition focusing on external personal skin patterns, hand geometry concentrating on personal hand shape and dimensions, retina scanning defining a person's unique blood vessel arrangement in the retina of the eye, voice verification distinguishing an individual's distinct sound waves, and signature verification.

Biometric applications may include but are not limited to, for instance physical access to restricted areas or applications; and access to computer systems containing sensitive information used by the military services, intelligence agencies, and other security-critical Federal organizations. Also, there are law enforcement applications which include home incarceration, parole programs, and physical access into jails or prisons. Also, government sponsored entitlement programs that rely on the Automated Fingerprint Identification System (AFIS) for access are important to deter fraud in social service programs by reducing duplicate benefits or even continued benefits after a recipient's demise.

Biometric recognition can be used in "identification mode", where the biometric system identifies a person from the entire enrolled population by searching a database for a match. A system can also be used in "verification mode", where the biometric  
5 system authenticates a person's claimed identity from his/her previously enrolled pattern of biometric data. In many biometric applications there is little margin for any inaccuracy in either the identification mode or the verification mode.

Current commercially available biometric methods and  
10 systems are limited because they use only externally visible distinguishing characteristics for identification; for example, fingerprints, iris patterns, hand geometry and blood vessel patterns. To date, the most widely used method is fingerprinting but there are several problems which have been encountered  
15 including false negative identifications due to dirt, moisture and grease on the print being scanned. Additionally, some individuals have insufficient detail of the ridge pattern on their print due to trauma or a wearing down of the ridge structure. More important, some individuals are reluctant to have their fingerprint patterns  
20 memorialized because of the ever increasing accessibility to personal information.

Other techniques, currently in use are iris pigment patterns and retina scanning. These methods are being introduced in many bank systems, but not without controversy. There are



health concerns that subjecting eyes to electromagnetic radiation may be harmful and could present unidentified risks.

Another limitation of current biometric systems, is the relative ease with which external physical features can be photographed, copied or lifted. This easy copying of external characteristics lends itself quite readily to unauthorized duplication of fingerprints, eye scans, and other biometric patterns. With the advancement of cameras, videos, lasers and synthetic polymers there is technology available to reproduce a human body part with the requisite unique physical patterns and traits of a particular individual. In high level security systems, where presentation of a unique skin or body pattern needs to be verified for entry, a counterfeit model could be produced, thereby allowing unauthorized entry into a secured facility by an imposter. As these capabilities evolve and expand there is a greater need to verify whether the body part offered for identification purposes is a counterfeit reproduction or the severed or lifeless body part of an authorized individual.

U.S. Patent No. 5,719,950 (Osten), incorporated by reference herein, suggests that verifying an exterior specific characteristic of an individual such as fingerprint in correlation with a non-specific characteristic such as oxygen level in the blood can determine if the person seeking authentication is actually present. This method may be effective but still relies on exterior characteristics for verification of the individual. Also,

the instrumentation is complicated having dual operations which introduce more variables to be checked before identity is verified.

Current biometric systems are also limited in size. For example, a fingerprint scanner must be at least as big as the  
5 fingerprint it is scanning. Other limitations include the lack of moldability and flexibility of some systems which prevents incorporation into flexible and moving objects. Finally, the complex scanning systems in current biometric methods are expensive and this high cost prevents the widespread use of these systems in  
10 all manner of keyless entry applications.

Accordingly, there is a need for more compact, moldable, flexible, economical and reliable automated biometric recognition methods and systems which use non-visible physical characteristics which are not easily copied, photographed, or duplicated. This  
15 would eliminate concerns regarding fingerprints that are unidentifiable due to dirt, grease, moisture or external surface deterioration; potential risks involved in eye scanning; costly instrumentation that depends on external characteristics, and the possibility of deceiving a system with an artificial reproduction  
20 of a unique external characteristic used for identification.

#### SUMMARY OF INVENTION

The present invention pertains to an apparatus for recognition of an individual living organism's identity. The

apparatus comprises a sensing mechanism for sensing electric and/or magnetic properties of the organism. The apparatus comprises a mechanism for recognizing the organism. The recognizing mechanism is in communication with the sensing mechanism.

5           The present invention pertains to a method for recognition of an individual living organism's identity. The method comprises the steps of sensing electric and/or magnetic properties of the organism. Then there is the step of recognizing the organism from the property.

10           The present invention pertains to an apparatus for recognition of an individual living organism's identity. The apparatus comprises a sensing mechanism having a contact area of less than 2.0 centimeters squared to identify an attribute of the organism. The sensing mechanism produces a signal corresponding to the attribute. The apparatus comprises a mechanism for recognizing  
15 the organism from the attribute. The sensing mechanism is in communication with the recognizing mechanism so the recognizing mechanism receives the signal from the sensing mechanism.

20           The present invention pertains to an apparatus for recognition of an individual living organism's identity. The apparatus comprises a sensing mechanism having a thickness of less than .2 centimeters to identify an attribute of the organism. The sensing mechanism produces a signal corresponding to the attribute. The apparatus comprises a mechanism for recognizing the organism

from the attribute. The sensing mechanism is in communication with the recognizing mechanism so the recognizing mechanism receives the signal from the sensing mechanism.

5 The present invention pertains to an apparatus for recognition of an individual living organism's identity. The apparatus comprises a sensing mechanism for sensing an attribute of the organism. The sensing mechanism produces a signal corresponding to the attribute. The apparatus comprises a mechanism for recognizing the organism from the attribute with an  
10 accuracy of greater than one in a billion.

15 The present invention pertains to an apparatus for recognition of an individual living organism's identity. The apparatus comprises a sensing mechanism which is moldable into a shape having a non-flat surface. The sensing mechanism senses an attribute of the organism and produces a signal corresponding to the attribute. The apparatus comprises a mechanism for recognizing the organism from the attribute. The recognizing mechanism is in communication with the sensing mechanism. In the preferred embodiment, the electrodes can be concave, flat, convex, or a  
20 combination thereof, lending them to molding into numerous devices. The electrode simply needs to touch the skin of the subject individual.

Characteristics of an organism can be detected by its electrical/magnetic properties, and an individual organism has unique electrical/magnetic properties.

5 I. The properties can be measured using any mechanism which measures the properties.

A. The properties can be measured using any mechanism which uses a DC, AC, electric field, magnetic field, and/or EM field.

10 B. The properties can be measured using touch and/or touchless methods.

C. The properties can be measured by positioning the organism in relation to the applied energy:

1. as part of an energy flow

15 2. interrupting an energy flow

3. responding to an energy field by generating its own energy flow

- The properties can be measured using induced currents.

20 D. The properties can be measured for a single body segment or for multiple segments. Multiple segments can be compared with each other, i.e., a measured segment from the left hand can be compared to a measured segment on  
25 the right hand.

- E. The properties can be measured using one or more frequencies.
- F. The properties can be measured using one or more waveform shapes.
- G. The properties can be measured generating 3 or more dimensional matrices.
- H. The properties can be measured using unique sensors.
  - 1. Size
  - 2. Flexibility
  - 3. Moldability
- I. The properties can be measured to one in one billion accuracy or greater.
- J. The properties can be measured by detecting energy emitted by the organism.

II. An individual organism can be recognized by its electrical/magnetic properties. Any of the mechanisms described in I. can be used for this. Although the absolute measurements will vary slightly from day to day, the relative ratios of the measurements will remain constant enough to derive a biometric pattern.

III. Diagnostic characteristics of an organism can be detected by its electrical/magnetic properties. Positioning the organism in relation to the applied

energy as part of an energy flow, interrupting an energy flow, and detecting emitted energy are described in the prior art. An organism responding to an energy field by generating its own energy flow, such as an induced current is not. Induced currents can be used to measure the electrical/magnetic properties of an organism to determine diagnostic characteristics such as:

- A. Presence or absence of bone trauma
- B. Presence or absence of tumors
- C. Presence or absence of toxins
- D. Levels of metabolites

The present invention pertains to an apparatus for identifying electric and/or magnetic properties of an individual living organism. The apparatus comprises a sensing mechanism for sensing the electric and/or magnetic properties. The apparatus comprises a mechanism for forming matrices corresponding to the organism having at least four-dimensions.

The present invention pertains to a method for sensing an induced current in an individual living organism. The method comprises the steps of inducing current in the organism. Then there is the step of detecting the current induced in the organism.

The present invention pertains to an apparatus for sensing an induced current in an individual living organism. The

apparatus comprises a mechanism for inducing current in the organism. The apparatus comprises a mechanism for detecting the current induced in the organism.

5 The present invention pertains to an apparatus for diagnosing a bone. The apparatus comprises a mechanism for inducing a current in the bone. The apparatus comprises a mechanism for detecting a fracture or break in the bone.

10 The present invention pertains to a method for diagnosing a bone. The method comprises the steps of inducing a current in the bone. Then there is the step of detecting the induced current in the bone. Next there is the step of detecting a fracture or break in the bone.

15 The present invention pertains to an apparatus for sensing the electric and/or magnetic properties of an individual living organism. The apparatus comprises a mechanism for transmitting electric and/or magnetic energy into the organism. The apparatus comprises a mechanism for receiving the electric and/or magnetic energy after it has passed through the organism.

20 The present invention pertains to a method for using a computer. The method comprises the steps of sensing a non-visible attribute of an individual. Then there is the step of recognizing the individual. Next there is the step of accessing the computer by the individual.



The present invention pertains to a method for secure communication between an individual at a first location and a second location. The method comprises the steps of sensing a non-visible attribute of an individual. Then there is the step of  
5 recognizing the individual. Next there is the step of allowing the individual to communicate with the second location.

The present invention pertains to an apparatus for authorizing an action. The apparatus comprises a mechanism for recognizing a biometric signature of an individual. The apparatus  
10 comprises a mechanism for allowing the action.

The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of the individual. Then there is the step of allowing the action to occur.

The present invention pertains to a method for conducting  
15 a financial transaction. The method comprises the steps of identifying a financial transaction which a person desires to execute. Then there is the step of recognizing a biometric signature of the person. Next there is the step of performing the  
20 financial transaction of the person.

The present invention pertains to a mechanism for charging a purchase. The mechanism comprises a mechanism for recognizing a biometric signature of a purchaser. The mechanism

comprises a mechanism for charging an account of the purchaser with the purchase price. The charging mechanism is connected to the recognizing mechanism.

5           The present invention pertains to a mechanism for authenticating an individual. The mechanism comprises a contact card having sensors which an individual touches to generate a biometric signature. The mechanism comprises a reader for the contact card for reading the contact card and recognizing the  
10 individual from the biometric signature.

          The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of the individual. Then there is the step of allowing the action to occur.

15           After the allowing step, there can be the step of performing the action.

          The present invention pertains to an apparatus for authorizing an action. The apparatus comprises a mechanism for recognizing a biometric signature of an individual. The apparatus  
20 comprises a mechanism for allowing the action.

          The action can be accessing an area, and the allowing mechanism preferably includes a mechanism for allowing access to the area.

The allowing mechanism can include a lock and a release mechanism connected to the recognizing mechanism and the lock. The recognizing mechanism produces a recognizing signal when the individual is recognized which is received by the release mechanism  
5 and causes the release mechanism to open the lock.

The area can be a database and the allowing mechanism includes a mechanism for allowing access to data in the database connected to the recognizing mechanism. The recognizing mechanism produces a recognizing signal when the individual is recognized  
10 which is received by the allowing access mechanism and causes the allowing access mechanism to allow the individual to access part or all of the database.

The allowing access mechanism can include a computer, a memory and an access program stored in the memory.

15 The apparatus can include a first account and a second account, and wherein the action is a financial transaction between the first account and the second account and the allowing mechanism includes a mechanism for allowing the financial transaction.

20 The allowing mechanism can allow the transfer of equities between the first account and the second account. The equities can include stocks or bonds.

The allowing mechanism can allow a transfer of money between the first account and the second account.

The apparatus can include a gambling mechanism which receives a bet and wherein the action includes placing a bet by the  
5 individual with the gambling mechanism and the recognizing mechanism is connected to the gambling mechanism and allows the gambling mechanism to place a bet it receives if the recognizing mechanism recognizes the individual.

The apparatus can include a telecommunication line  
10 connected to the gambling mechanism over which the bet is sent to the gambling mechanism. The recognizing mechanism can include a card with sensors for the individual to touch which provides the biometric signature.

The apparatus can include a utility box and wherein the  
15 action includes accessing the utility box, and the recognizing mechanism is connected to the utility box and allows access to the utility box when a recognizing mechanism recognizes the individual. The utility box can include a transmitter which transmits a usage reading when the biometric signature is recognized.

20 The action can include paying a fee, and the apparatus can include a memory having an account of the individual, and a mechanism for charging the account of the individual the fee when said recognizing mechanism recognizes the individual. The

recognizing mechanism is connected to the charging mechanism. The charging mechanism is connected to the memory.

The fee can be for accessing a subway or a turnpike or a bus, or other vehicle or vehicular route.

5           The apparatus can include a phone and the action includes making a call on the phone, and the recognizing mechanism is connected to the phone and allows a call to be made on the phone when a recognizing mechanism recognizes the individual. The phone can have a hand piece with sensors through which the biometric  
10           signature of the individual is received.

The recognizing mechanism can include a card with sensors for the individual to touch which provides the biometric signature.

          The apparatus can include a video phone and wherein the action includes making a call on the video phone and the  
15           recognizing mechanism is connected to the video phone and allows a call to be made by the individual on the video phone when the recognizing mechanism recognizes the individual.

          The apparatus can include a television and wherein the action includes activating the television or a channel of the  
20           television, and the recognizing mechanism is connected to the television and allows the television or channel to be activated by

the individual when the recognizing mechanism recognizes the individual.

The apparatus can include a lock-out box connected to the television and the recognizing mechanism through which the channel  
5 passes to the television, and the recognizing mechanism includes sensors through which the biometric signature of the individual is received.

The recognizing mechanism can include a card with sensors for the individual to touch which provides the biometric signature.

10 The recognizing mechanism can include a touchless electric field sensor for measuring induced current in the individual to obtain the biometric signature, and wherein the card has a memory which stores a known biometric signature of the individual, and wherein the recognizing mechanism has a reader for  
15 obtaining the known biometric signature from the card.

The apparatus can include a check-out box mechanism for checking out a book, and the action is checking out the book from a library, and the recognizing mechanism is connected to the check-out box mechanism and allows the book to be checked out when  
20 the recognizing mechanism recognizes the individual.

The apparatus can include an airline gate counter, and the action is boarding a plane, and the recognizing mechanism is

connected to the airline gate counter and allows the individual to board the plane when the recognizing mechanism recognizes the biometric signature of the individual.

5 The apparatus can include a memory stick in which is stored a known biometric signature of the individual and account information of the individual, and a memory stick reader connected to the recognizing mechanism, said recognizing mechanism reading the biometric signature of the individual and comparing it to the known biometric signature of the individual from the memory stick.

10 The apparatus can include an electronic passport having a known biometric signature of the individual, and a passport reader, and the action is passing through customs, and the recognizing mechanism is connected to the passport reader and allows the individual through customs when the recognizing  
15 mechanism recognizes the individual.

The apparatus can include a card having a microchip and sensors for obtaining the biometric signature, and a cash register with a card reader which reads the card to obtain the biometric signature, and applies a purchase price to the card if the  
20 individual is recognized, said recognizing mechanism is connected to the cash register. The recognizing mechanism can include a touchless device measuring magnetic properties via reflected electromagnetic waves from the individual to identify the biometric signature, and including a cash register connected to the

recognizing mechanism which charges the purchase to an account of the individual when the recognizing mechanism recognizes the individual.

5 The apparatus can include a driver's license having a known biometric signature of the individual and sensors for obtaining the biometric signature of the individual, and a car having the recognizing mechanism which includes a reader for the license, said reader applying a traffic offense to the individual's license. The action can include accessing a room having computer  
10 terminals, and including a door lock to a door to the room and the recognizing mechanism is connected to the door lock and unlocks the door when the recognizing mechanism recognizes the individual. The recognizing mechanism can produce a multi-frequency acoustic field scan to produce alternating current in the individual to obtain the  
15 biometric signature.

The apparatus can include an identification card having the biometric signature of the individual, and a microprocessor.

The apparatus can include a time clock, a memory having an account of the individual. The recognizing mechanism is  
20 connected to the time clock and records a time the individual communicates with the recognizing mechanism.

The apparatus can include a memory having data of a patient, a terminal which connects to the memory and the



recognizing mechanism connected to the terminal. The terminal accesses medical records of the patient when the recognizing mechanism recognizes the biometric signature of the individual. The terminal can be a notepad.

5           The apparatus can include a PAN wrist device synchronizing cellular phone, pager and personal digital assistant capabilities and which provides the biometric signature of the individual, and a personal area network. The wrist device accesses the personal area network when the recognizing mechanism, which is  
10 connected to the terminal, recognizes the individual.

          The apparatus can include a card with sensors and a microchip which contains data concerning government services value, and the biometric signature of the individual. The government services value is lowered when the card contacts the recognizing  
15 mechanism and the recognizing mechanism recognizes the individual.

          The apparatus can include a biometric glove for obtaining the biometric signature of the individual, and electronic records which are accessed by the individual as long as the individual wears the biometric glove and the recognizing mechanism to which  
20 the glove is connected, recognizes the individual.

          The apparatus can include a software program which is activated by the biometric signature of the individual and a memory in which the software program is stored. The recognizing mechanism

is connected to the memory. The software program can require the biometric signature to be received at predetermined periods of time for continuous operation of the software program.

5 The apparatus can include an electronic lock and a door to a room to which the lock is connected. The recognizing mechanism is connected to the lock which allows the lock to open when the recognizing mechanism recognizes the individual.

10 The apparatus can include a door having a door handle having biometric electrodes that obtain the biometric signature of the individual when the individual grabs the handle, and a memory. The recognizing mechanism records in the memory the identity of the individual and the time and date the individual contacted the door handle.

15 The apparatus can include a computer having a memory having sections. The sections restricted and being accessed only with a predetermined biometric signature. The recognizing mechanism is connected to the computer.

20 The apparatus can include a door having a door handle with biometric sensors, and a lock which is allowed to open when the biometric signature of the individual is recognized by the recognizing mechanism. The recognizing mechanism is connected to the door handle and the lock. The apparatus can include a mechanism which mechanically produces electricity connected to the sensors.

The apparatus can include a weapon which performs a defensive function and has biometric sensors, and in which the recognizing mechanism is disposed and is connected to the biometric sensors and the trigger of the weapon, so the trigger can only be  
5 activated when the biometric signature of the individual is recognized.

The apparatus can include a touch electrode wrist band that is worn by the individual, and a portable recognizing mechanism to which the wrist band communicates to provide the  
10 biometric signature of the individual to the recognizing mechanism.

The apparatus can include a pharmacy cabinet for holding drugs, and a door with a lock. The recognizing mechanism is connected to the lock and unlocks the lock when the recognizing mechanism recognizes the individual so the individual can open the  
15 door to the cabinet. The apparatus can include a recording mechanism connected to the recognizing mechanism which records the date, time and individual's identity each time the door is unlocked.

The apparatus can include a pharmacy cabinet having drugs  
20 in it, and a door with a lock, including a PAN sensor card having the biometric signature of the individual, and the recognizing mechanism includes a receiver for receiving the biometric signature from the PAN sensor card. The recognizing mechanism is connected

to the lock and unlocks the lock when the recognizing mechanism recognizes the biometric signature of the individual.

The apparatus can include a memory having electronic records, a forehead mounted headset fitted with virtual screen  
5 glasses having see through mode which allows the individual to view actual reality and virtual records at the same time through the glasses. The headset has sensors for obtaining the biometric signature of the individual. The headset having a transmitter for transmitting the biometric signature to the recognizing mechanism.

10 The headset having a receiver which receives the electronic records when the recognizing mechanism recognizes the biometric signature of the individual.

The apparatus can include a telecommunications switching system, a cabinet in which this system is disposed. The cabinet  
15 having a door with a lock. The recognizing mechanism connected to the lock, and including a contactless smart card having the biometric signature of the individual which communicates with the recognizing mechanism. The recognizing mechanism causes the lock to open when the biometric signature of the individual is  
20 recognized.

The apparatus can include an ATM machine which holds and dispenses cash having a door and a lock. The recognizing mechanism connected to the lock, and a sensor card which contacts the recognizing mechanism and provides the biometric signature to the

recognizing mechanism when the individual touches the sensor card. The recognizing mechanism allowing the lock to open when the recognizing mechanism recognizes the individual's biometric signature.

5           The apparatus can include a vehicle having a door handle and steering wheel, either or both of which have biometric sensors. The recognizing mechanism is connected to the sensors in the door handle with the sensors and allowing the door handle to open the door, or the sensors in the steering wheel with the sensors  
10 allowing the engine to start when the recognizing mechanism recognizes the biometric signature from the respective sensors.

          The apparatus can include a vehicle having a battery, and a motor and a key entry connected to the recognizing mechanism, and a key having sensors for insertion into the key entry by the  
15 individual. The key when inserted into the key entry receives current from the battery to obtain the biometric signature of the individual. The recognizing mechanism connected to the motor and allowing the motor to engage when the recognizing mechanism recognizes the individual.

20           The apparatus can include a remote controller having biometric sensors and the recognizing mechanism for recognizing the biometric signature of the individual and allowing the controller to transmit a control signal.

The apparatus can include an ankle band with biometric sensors and a transmitter which transmits the biometric signature of the individual obtained from the sensor. The recognizing mechanism including a receiver for receiving the transmitted  
5 biometric signature, and an alarm which is triggered by the recognizing mechanism if the recognizing mechanism does not receive the biometric signature transmitted by the transmitter at a predetermined time.

The apparatus can include a wrist band having a unique ID  
10 and biometric sensors for obtaining the biometric signature of the individual wearing the wrist band, and having a wrist band transmitter/receiver, and wherein the recognizing mechanism has a recognizing transmitter/receiver which communicates with the wrist band transmitter/receiver for determining where the wrist band is  
15 located and for recognizing the individual wearing the wrist band.

The apparatus can include a GPS system and including a controller PAN touch sensor card for providing the biometric signature of the individual obtaining the PAN touch sensor card and a transmitter/receiver for communicating the biometric signature  
20 and other information to the recognizing mechanism and the GPS. The recognizing mechanism having a recognizing transmitter/receiver which communicates with the GPS and the PAN transmitter/receiver for recognizing the individual, ascertaining the position of the individual from the GPS and receiving the other information.

The present invention pertains to a method for charging a purchase. The method comprises the steps of recognizing a biometric signature of a purchaser. Then there is the step of charging an account of the purchaser with the purchase price.

5           The present invention pertains to a method for charging a purchase. The method comprises the steps of recognizing a biometric signature of a purchaser using a sensor mechanism with unique characteristics. Then there is the step of charging an account of the purchaser with the purchase price.

10           The present invention pertains to a method for charging a purchase. The method comprises the steps of recognizing a biometric signature of a purchaser using a sensor mechanism sensing acoustic characteristics. Then there is the step of charging an account of the purchaser with the purchase price.

15           The present invention pertains to a method for charging a purchase. The method comprises the steps of recognizing a biometric signature of a purchaser using a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of charging an account of the purchaser with the purchase price.

20           The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching sensors of a card by the individual to generate a biometric signature of the individual. Then there is the step of

reading the card with a reader and recognizing the individual from the biometric signature.

5 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a card having sensors with a unique characteristic by the individual to generate a biometric signature. Then there is the step of reading the card with a reader and recognizing the individual from the biometric signature.

10 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a card having sensors for sensing acoustic characteristics by the individual to generate a biometric signature. Then there is the step of reading the card with a reader and recognizing the individual from the biometric signature.

15 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a card having sensors for sensing an electric and/or magnetic characteristic by the individual to generate a biometric signature. Then there is the step of reading the card with a  
20 reader and recognizing the individual from the biometric signature.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching sensors of a memory stick by the individual to generate a



biometric signature of the individual. Then there is the step of reading the memory stick with a reader and recognizing the individual from the biometric signature.

5 The present invention pertains to a method for authorizing an action. The method comprises the steps of placing a memory stick in which is stored a known biometric signature of the individual into a memory stick reader connected to a recognizing mechanism. Then there is the step of reading the biometric signature of the individual. Next there is the step of  
10 comparing it to the known biometric signature of the individual from the memory stick with the recognizing mechanism to recognize the biometric signature of the individual. Then there is the step of recognizing a biometric signature of an individual. Next there is the step of allowing the action when the recognizing mechanism  
15 recognizes the biometric signature of the individual.

The present invention pertains to a method for authorizing an action. The method comprises the steps of placing a memory stick in which is stored a known biometric signature of the individual of the individual into a memory stick reader  
20 connected to a recognizing mechanism. Then there is the step of reading the biometric signature of the individual having a sensor mechanism with unique characteristics. Next there is the step of comparing it to the known biometric signature of the individual from the memory stick with the recognizing mechanism to recognize  
25 the biometric signature of the individual. Then there is the step

of recognizing a biometric signature of an individual. Next there is the step of allowing the action when the recognizing mechanism recognizes the biometric signature of the individual.

5 The present invention pertains to a method for authorizing an action. The method comprises the steps of placing a memory stick in which is stored a known biometric signature of the individual of the individual into a memory stick reader connected to a recognizing mechanism. Then there is the step of reading the biometric signature of the individual with a sensor  
10 mechanism for sensing an acoustic characteristic. Next there is the step of comparing it to the known biometric signature of the individual from the memory stick with the recognizing mechanism to recognize the biometric signature of the individual. Then there is the step of recognizing a biometric signature of an individual.  
15 Next there is the step of allowing the action when the recognizing mechanism recognizes the biometric signature of the individual.

The present invention pertains to a method for authorizing an action. The method comprises the steps of placing a memory stick in which is stored a known biometric signature of  
20 the individual into a memory stick reader connected to a recognizing mechanism. Then there is the step of reading the biometric signature of the individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Next there is the step of comparing it to the known biometric signature of the  
25 individual from the memory stick with the recognizing mechanism to

recognize the biometric signature of the individual. Then there is the step of recognizing a biometric signature of an individual. Next there is the step of allowing the action when the recognizing mechanism recognizes the biometric signature of the individual.

5           The present invention pertains to a method for accessing an area. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing access to the area when the biometric signature of the individual is recognized.

10           The present invention pertains to a method for accessing an area. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an acoustic characteristic. Then there is the step of allowing access to the area when the biometric signature of the individual is  
15 recognized.

          The present invention pertains to a method for accessing an area. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of  
20 allowing access to the area when the biometric signature of the individual is recognized.

          The present invention pertains to a method for accessing a database. The method comprises the steps of recognizing a

biometric signature of an individual. Then there is the step of producing a recognizing signal when the individual is recognized. Next there is the step of receiving by an allowing access mechanism the recognizing signal which causes the allowing access mechanism  
5 to allow the individual to access part or all of the database.

The present invention pertains to a method for accessing a database. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of producing a  
10 recognizing signal when the individual is recognized. Next there is the step of receiving by an allowing access mechanism the recognizing signal which causes the allowing access mechanism to allow the individual to access part or all of the database.

The present invention pertains to a method for accessing  
15 a database. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of producing a recognizing signal when the individual is recognized. Next there is the step of receiving by an allowing access mechanism  
20 the recognizing signal which causes the allowing access mechanism to allow the individual to access part or all of the database.

The present invention pertains to a method for accessing a database. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism

sensing an electric and/or magnetic characteristic. Then there is the step of producing a recognizing signal when the individual is recognized. Next there is the step of receiving by an allowing access mechanism the recognizing signal which causes the allowing  
5 access mechanism to allow the individual to access part or all of the database.

The present invention pertains to a method for authorizing a financial transaction. The method comprises the steps of recognizing a biometric signature of an individual with a  
10 sensor mechanism having a unique characteristic. Then there is the step of allowing the financial transaction when the biometric signature of the individual is recognized.

The present invention pertains to a method for authorizing a financial transaction between a first account and a  
15 second account. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an acoustic characteristic. Then there is the step of allowing the financial transaction when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for authorizing a financial transaction between a first account and a second account. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is

the step of allowing the financial transaction when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for gambling. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of placing a bet by the individual when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for gambling. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism having a unique characteristic. Then there is the step of placing a bet by the individual when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for gambling. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism for sensing an acoustic characteristic. Then there is the step of placing a bet by the individual when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for gambling. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of placing

a bet by the individual when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for gaming. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of playing a game by the individual when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for gaming. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism having a unique characteristic. Then there is the step of playing a game by the individual when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for gaming. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism for sensing an acoustic characteristic. Then there is the step of playing a game by the individual when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for gaming. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of playing

a game by the individual when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for accessing a utility box. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of allowing access to the utility box when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for accessing a utility box. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing access to the utility box when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for accessing a utility box. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an acoustic characteristic. Then there is the step of allowing access to the utility box when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for accessing a utility box. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is



the step of allowing access to the utility box when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for accessing a meter. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of allowing access to the meter when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for accessing a meter. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing access to the meter when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for accessing a meter. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an acoustic characteristic. Then there is the step of allowing access to the meter when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for accessing a meter. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step

of allowing access to the meter when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for paying a fee. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of charging an account of the individual the fee when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for paying a fee. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of charging an account of the individual the fee when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for paying a fee. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an acoustic characteristic. Then there is the step of charging an account of the individual the fee when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for paying a fee. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of

charging an account of the individual the fee when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for accessing a vehicle or vehicular route. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of allowing access to the vehicle or vehicular route when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for accessing a vehicle or vehicular route. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing access to the vehicle or vehicular route when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for accessing a vehicle or vehicular route. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of allowing access to the vehicle or vehicular route when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for accessing a vehicle or vehicular route. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then

there is the step of allowing access to the vehicle or vehicular route when the biometric signature of the individual is recognized.

The present invention pertains to a method for using a telecommunications apparatus for a communication. The method  
5 comprises the steps of recognizing a biometric signature of an individual. Then there is the step of allowing the communication with the telecommunications apparatus when the individual is recognized.

The present invention pertains to a method for using a  
10 telecommunications apparatus for a communication. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing the communication with the telecommunications apparatus when the individual is recognized.

The present invention pertains to a method for using a  
15 telecommunications apparatus for a communication. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of allowing the  
20 communication with the telecommunications apparatus when the individual is recognized.

The present invention pertains to a method for using a telecommunications apparatus for a communication. The method

comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of allowing the communication with the telecommunications apparatus when the  
5 individual is recognized.

The present invention pertains to a method for watching a television. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of activating a television and/or channel of the television when the  
10 individual is recognized.

The present invention pertains to a method for watching a television. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of activating a  
15 television and/or channel of the television when the individual is recognized.

The present invention pertains to a method for watching a television. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism  
20 sensing an acoustic characteristic. Then there is the step of activating a television and/or channel of the television when the individual is recognized.

The present invention pertains to a method for watching a television. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is  
5 the step of activating a television and/or channel of the television when the individual is recognized.

The present invention pertains to a method for checking out a book. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of  
10 checking out a book with a check-out box mechanism when the individual is recognized.

The present invention pertains to a method for checking out a book. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having  
15 a unique characteristic. Then there is the step of checking out a book with a check-out box mechanism when the individual is recognized.

The present invention pertains to a method for checking out a book. The method comprises the steps of recognizing a  
20 biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of checking out a book with a check-out box mechanism when the individual is recognized.

The present invention pertains to a method for checking out a book. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is  
5 the step of checking out a book with a check-out box mechanism when the individual is recognized.

The present invention pertains to a method for boarding a plane. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of allowing the  
10 individual to pass through a gate to board the plane when the biometric signature of the individual is recognized.

The present invention pertains to a method for boarding a plane. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique  
15 characteristic. Then there is the step of allowing the individual to pass through a gate to board the plane when the biometric signature of the individual is recognized.

The present invention pertains to a method for boarding a plane. The method comprises the steps of recognizing a biometric  
20 signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of allowing the individual to pass through a gate to board the plane when the biometric signature of the individual is recognized.

The present invention pertains to a method for boarding a plane. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of  
5 allowing the individual to pass through a gate to board the plane when the biometric signature of the individual is recognized.

The present invention pertains to a method for passing through customs. The method comprises the steps of reading a known biometric signature of an individual from an electronic passport  
10 having a known biometric signature of the individual. Next there is the step of recognizing the biometric signature of the individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing the individual through customs when the biometric signature of the individual is recognized from  
15 the known biometric signature of the individual.

The present invention pertains to a method for passing through customs. The method comprises the steps of reading a known biometric signature of an individual from an electronic passport having a known biometric signature of the individual. Next there  
20 is the step of recognizing the biometric signature of the individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of allowing the individual through customs when the biometric signature of the individual is recognized from the known biometric signature of the individual.



The present invention pertains to a method for passing through customs. The method comprises the steps of reading a known biometric signature of an individual from an electronic passport having a known biometric signature of the individual. Next there  
5 is the step of recognizing the biometric signature of the individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of allowing the individual through customs when the biometric signature of the individual is recognized from the known biometric signature of the  
10 individual.

The present invention pertains to a method for applying a traffic citation or offense to an individual's license and record. The method comprises the steps of reading a known biometric signature of the individual from a driver's license  
15 having a known biometric signature of the individual. Next there is the step of recognizing a biometric signature of an individual. Then there is the step of recording the traffic citation or offense on the individual's license and record when the biometric signature of the individual is recognized from the known biometric signature  
20 of the individual.

The present invention pertains to a method for applying a traffic citation or offense to an individual's license and record. The method comprises the steps of reading a known biometric signature of the individual from a driver's license  
25 having a known biometric signature of the individual. Next there

is the step of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of recording the traffic citation or offense on the individual's license and record when the biometric signature of the individual is recognized from the known biometric signature of the individual.

The present invention pertains to a method for applying a traffic citation or offense to an individual's license and record. The method comprises the steps of reading a known biometric signature of the individual from a driver's license having a known biometric signature of the individual. Next there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of recording the traffic offense on the individual's license and record when the biometric signature of the individual is recognized from the known biometric signature of the individual.

The present invention pertains to a method for applying a traffic citation or offense to an individual's license and record. The method comprises the steps of reading a known biometric signature of the individual from a driver's license having a known biometric signature of the individual. Next there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of recording the traffic

citation or offense on the individual's license and record when the biometric signature of the individual is recognized from the known biometric signature of the individual.

5 The present invention pertains to a method for accessing a room having computer terminals. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of unlocking a door to the room with the computer terminals when the individual is recognized.

10 The present invention pertains to a method for accessing a room having computer terminals. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of unlocking a door to the room with the computer terminals  
15 when the individual is recognized.

The present invention pertains to a method for accessing a room having computer terminals. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then  
20 there is the step of unlocking a door to the room with the computer terminals when the individual is recognized

The present invention pertains to a method for monitoring when an individual performs an action. The method comprises the

steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of a memory having an account of the individual, the recognizing mechanism recording a time in an account of the individual when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for monitoring when an individual performs an action. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of a memory having an account of the individual, the recognizing mechanism recording a time in an account of the individual when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for monitoring when an individual performs an action. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of a memory having an account of the individual, the recognizing mechanism recording a time in an account of the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing an account of an individual. The method comprises the steps of

recognizing a biometric signature of an individual. Next there is the step of allowing access of the account of the when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for accessing an account of an individual. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of allowing access of the account of the individual through a terminal when the biometric signature of the individual is  
10 recognized.

15 The present invention pertains to a method for accessing an account of an individual. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of allowing access of the account of the individual through a terminal when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for accessing an account of an individual. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of allowing access of the account of the individual through a terminal when the biometric signature of the individual is recognized.



1. The first step is to identify the problem or question that needs to be addressed. This involves understanding the context and the specific requirements of the task.

9

characteristic. Next there is the step of lowering a value of benefits or funds in an account of the individual when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a locking mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing a biometric signature of the individual. Next there is the step of opening the locking mechanism to access the area.

10 The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a locking mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing a biometric signature of the individual with a sensor mechanism  
15 having a unique characteristic. Then there is the step of opening the locking mechanism to access the area.

The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a locking mechanism to the area to obtain the biometric  
20 signature of the individual. Next there is the step of recognizing a biometric signature of the individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of opening the locking mechanism to access the area.

The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a locking mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing  
5 a biometric signature of the individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of opening the locking mechanism to access the area.

10 The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a handle having a sensor of an entry mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing a biometric signature of the individual. Next there is the step of opening the locking mechanism to access the area.

15 The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a handle, having a sensor mechanism having a unique characteristic, of an entry mechanism to the area to obtain the biometric signature of the individual. Next there is the step of  
20 recognizing a biometric signature of the individual. Then there is the step of opening the locking mechanism to access the area.

The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a handle, having a sensor mechanism sensing an acoustic



characteristic, of an entry mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing a biometric signature of the individual. Then there is the step of opening the locking mechanism to access the area.

5           The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a handle, having a sensor mechanism sensing an electric and/or magnetic characteristic, of an entry mechanism to the area to obtain the biometric signature of the individual. Next there is  
10 the step of recognizing a biometric signature of the individual. Then there is the step of opening the locking mechanism to access the area.

15           The present invention pertains to a method for accessing data. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of accessing only authorized sections of a memory or data storage mechanism by an individual when the biometric signature of the individual is recognized.

20           The present invention pertains to a method for accessing data. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of accessing only authorized sections of a memory or data storage mechanism by an

individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing data. The method comprises the steps of recognizing a biometric  
5 signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of accessing only authorized sections of a memory or data storage mechanism by an individual when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for accessing data. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of accessing only authorized sections of a memory or data storage  
15 mechanism by an individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing a network. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of  
20 accessing only authorized sections of the network with a network access mechanism when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing a network. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of accessing only  
5 authorized sections of the network with a network access mechanism when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing a network. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism  
10 sensing an acoustic characteristic. Next there is the step of accessing only authorized sections of the network with a network access mechanism when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing  
15 a network. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of accessing only authorized sections of the network with a network access mechanism when the biometric signature of the  
20 individual is recognized.

The present invention pertains to a method for accessing software. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of

accessing the software when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing software. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of accessing the software when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing software. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of accessing the software when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing software. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of accessing the software when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing a computer. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of

accessing the computer when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for accessing a computer. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of accessing the computer when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for accessing a computer. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of accessing the computer when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for accessing a computer. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of accessing the computer when the biometric signature of  
20 the individual is recognized.

The present invention pertains to a method for protection. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of

activating a weapon when the biometric signature of the individual is recognized, said recognizing mechanism integral to the weapon.

5 The present invention pertains to a method for protection. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of activating a weapon when the biometric signature of the individual is recognized, said recognizing mechanism integral to the weapon.

10 The present invention pertains to a method for protection. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of activating a weapon when the biometric signature of the individual is recognized, said recognizing mechanism integral to the weapon.

15 The present invention pertains to a method for protection. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of activating a weapon when the biometric signature of the individual is recognized, said recognizing mechanism integral to the weapon.

20

The present invention pertains to a method for accessing drugs. The method comprises the steps of recognizing a biometric

signature of an individual. Next there is the step of unlocking a lock of an area for holding drugs when the biometric signature of the individual is recognized so the individual can open the door to the area.

5           The present invention pertains to a method for accessing drugs. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of unlocking a lock of an  
10 individual is recognized so the individual can open the door to the area.

          The present invention pertains to a method for accessing drugs. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an  
15 acoustic characteristic. Next there is the step of unlocking a lock of an area for holding drugs when the biometric signature of the individual is recognized so the individual can open the door to the area.

          The present invention pertains to a method for accessing  
20 drugs. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of unlocking a lock of an area for holding drugs when the biometric

signature of the individual is recognized so the individual can open the door to the area.

5 The present invention pertains to a method for recognizing an individual. The method comprises the steps of sensing with sensors of a forehead mounted headset on an individual a biometric signature of an individual. Then there is the step of recognizing the individual from the biometric signature of the individual.

10 The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors of a forehead mounted headset on an individual a biometric signature of an individual. Then there is the step of recognizing the biometric signature of the individual with the recognizing mechanism with a sensor mechanism having a unique characteristic.

15 The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors of a forehead mounted headset on an individual a biometric signature of an individual. Then there is the step of recognizing the biometric signature of the individual with the recognizing  
20 mechanism with a sensor mechanism sensing an acoustic characteristic.

The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with



sensors of a forehead mounted headset on an individual a biometric signature of an individual. Then there is the step of recognizing the biometric signature of the individual with the recognizing mechanism with a sensor mechanism sensing an electric and/or  
5 magnetic characteristic.

The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors of a forehead mounted headset on an individual a biometric signature of an individual. Next there is the step of transmitting  
10 the biometric signature of the individual with a transmitter on the headset. Next there is the step of receiving the transmitted biometric signature of the individual at a recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual with the recognizing mechanism communicating with  
15 the forehead sensor. Then there is the step of allowing access by the individual to the electronic records.

The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors having a unique characteristic of a forehead mounted  
20 headset on an individual a biometric signature of an individual. Next there is the step of transmitting the biometric signature of the individual with a transmitter on the headset. Next there is the step of receiving the transmitted biometric signature of the individual at a recognizing mechanism. Next there is the step of  
25 recognizing the biometric signature of the individual with the

recognizing mechanism communicating with the forehead sensor with a sensor mechanism having a unique characteristic. Then there is the step of allowing access by the individual to the electronic records.

5           The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors sensing acoustic characteristics of a forehead mounted headset on an individual a biometric signature of an individual. Next there is the step of transmitting the biometric signature of  
10 the individual with a transmitter on the headset. Next there is the step of receiving the transmitted biometric signature of the individual at a recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual with the recognizing mechanism communicating with the forehead sensor with  
15 a sensor mechanism sensing an acoustic characteristic. Then there is the step of allowing access by the individual to the electronic records.

          The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with  
20 sensors for sensing electric and/or magnetic characteristics of a forehead mounted headset on an individual a biometric signature of an individual. Next there is the step of transmitting the biometric signature of the individual with a transmitter on the headset. Next there is the step of receiving the transmitted  
25 biometric signature of the individual at a recognizing mechanism.

Next there is the step of recognizing the biometric signature of the individual with the recognizing mechanism communicating with the forehead sensor with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of allowing  
5 access by the individual to the electronic records.

The present invention pertains to a method for accessing equipment. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of unlocking a lock to an area with the equipment disposed in it or to  
10 the equipment itself when the biometric signature of the individual is recognized so the individual can enter the area.

The present invention pertains to a method for accessing equipment. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism  
15 sensing an electric and/or magnetic characteristic. Next there is the step of unlocking a lock to an area with the equipment disposed in it or to the equipment when the biometric signature of the individual is recognized so the individual can enter the area.

The present invention pertains to a method for accessing  
20 equipment. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of unlocking a lock to an area with the equipment disposed in it or to the

equipment itself when the biometric signature of the individual is recognized so the individual can enter the area.

The present invention pertains to a method for accessing equipment. The method comprises the steps of recognizing a  
5 biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of unlocking a lock to an area with the equipment disposed in it or to the equipment itself when the biometric signature of the individual is recognized so the individual can enter the area.

10 The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of unlocking a lock mechanism of an ATM machine which holds and dispenses cash when the  
15 biometric signature of the individual is recognized so the individual can access the ATM machine.

20 The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of unlocking a lock mechanism of an ATM machine which holds and dispenses cash when the biometric signature of the individual is recognized so the individual can access the ATM machine.

The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of  
5 unlocking a lock mechanism of an ATM machine which holds and dispenses cash when the biometric signature of the individual is recognized so the individual can access the ATM machine.

The present invention pertains to a method for operating a vehicle or craft. The method comprises the steps of recognizing  
10 the biometric signature of the individual. Then there is the step of allowing the operation of the vehicle when the biometric signature of the individual is recognized.

The present invention pertains to a method for entering a vehicle or craft. The method comprises the steps of touching a  
15 door handle of a door of the vehicle having a sensor to obtain a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual with a sensor mechanism having a unique characteristic. Next there is the step of unlocking a door lock of a vehicle when the biometric signature  
20 of the individual is recognized.

The present invention pertains to a method for entering a vehicle or craft. The method comprises the steps of touching a door handle of a door of the vehicle having a sensor to obtain a biometric signature of an individual. Next there is the step of

recognizing the biometric signature of the individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of unlocking a door lock of a vehicle when the biometric signature of the individual is recognized.

5           The present invention pertains to a method for entering a vehicle or craft. The method comprises the steps of touching a door handle of a door of the vehicle having a sensor to obtain a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual with a sensor  
10 mechanism sensing an electric and/or magnetic characteristic. Next there is the step of unlocking a door lock of a vehicle when the biometric signature of the individual is recognized.

15           The present invention pertains to a method for operating a vehicle. The method comprises the steps of inserting a key into a key entry of a vehicle. Then there is the step of recognizing a biometric signature of an individual. Next there is the step of engaging a motor or engine of the vehicle when the biometric signature of the individual is recognized and the key is inserted in the key entry.

20           The present invention pertains to a method for operating a vehicle. The method comprises the steps of inserting a key into a key entry of a vehicle. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of engaging a

motor or engine of the vehicle when the biometric signature of the individual is recognized and the key is inserted in the key entry.

5 The present invention pertains to a method for operating a vehicle. The method comprises the steps of inserting a key into a key entry of a vehicle. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of engaging a motor or engine of the vehicle when the biometric signature of the individual is recognized and the key is inserted  
10 in the key entry.

15 The present invention pertains to a method for operating a vehicle. The method comprises the steps of inserting a key into a key entry of a vehicle. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of engaging a motor or engine of the vehicle when the biometric signature of the individual is recognized and the key is inserted in the key entry.

20 The present invention pertains to a method for accessing an area. The method comprises the steps of inserting a key into a key entry of a lock to the area. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism in communication with the key. Next there is the step of

opening the lock when the biometric signature of the individual is recognized and the key is inserted in the key entry.

5 The present invention pertains to a method for accessing an area. The method comprises the steps of inserting a key into a key entry of a lock to the area. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic in communication with the key. Next there is the step of opening the lock when the biometric signature of the individual is recognized and the key is inserted  
10 in the key entry.

15 The present invention pertains to a method for accessing an area. The method comprises the steps of inserting a key into a key entry of a lock to the area. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic in communication with the key. Next there is the step of opening the lock when the biometric signature of the individual is recognized and the key is inserted in the key entry.

20 The present invention pertains to a method for accessing an area. The method comprises the steps of inserting a key into a key entry of a lock to the area. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic in communication with the key. Next there is the step of opening the



lock when the biometric signature of the individual is recognized and the key is inserted in the key entry.

The present invention pertains to a method for activating a control signal. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of producing a control signal with a transmitter for transmitting the control signal of a remote controller when the biometric signature of the individual is recognized.

The present invention pertains to a method for activating a control signal. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of producing a control signal with a transmitter for transmitting the control signal of a remote controller when the biometric signature of the individual is recognized.

The present invention pertains to a method for activating a control signal. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of producing a control signal with a transmitter for transmitting the control signal of a remote controller when the biometric signature of the individual is recognized.

The present invention pertains to a method for activating a control signal. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is  
5 the step of producing a control signal with a transmitter for transmitting the control signal of a remote controller when the biometric signature of the individual is recognized.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a  
10 biometric signature of an individual from a transmitter of a mechanism of a wearing mechanism worn by an individual, said mechanism for obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Next there is  
15 the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signal of an individual from a transmitter of a mechanism  
20 with a sensor mechanism having a unique characteristic of a wearing mechanism worn by an individual, said mechanism for obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Next there is the step of recognizing  
25 the biometric signature of the individual received at the receiver.

663044  
The present invention pertains to a method for  
monitoring. The method comprises the steps of transmitting a  
biometric signal of an individual from a transmitter of a mechanism  
with a sensor mechanism sensing an acoustic characteristic of a  
5 wearing mechanism worn by an individual, said mechanism for  
obtaining the biometric signature of the individual. Next there is  
the step of receiving the biometric signature with a receiver at a  
location remote from the transmitter. Then there is the step of  
recognizing the biometric signature of the individual received at  
10 the receiver.

663044  
The present invention pertains to a method for  
monitoring. The method comprises the steps of transmitting a  
biometric signal of an individual from a transmitter of a mechanism  
with a sensor mechanism sensing an electric and/or magnetic  
15 characteristic of a wearing mechanism worn by an individual, said  
mechanism for obtaining the biometric signature of the individual.  
Next there is the step of receiving the biometric signature with a  
receiver at a location remote from the transmitter. Then there is  
the step of recognizing the biometric signature of the individual  
20 received at the receiver.

The present invention pertains to a method for  
monitoring. The method comprises the steps of transmitting a  
biometric signature of an individual from a transmitter of a  
mechanism of a wearing mechanism worn by an individual, said  
25 mechanism for obtaining the biometric signature of the individual.

Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

5           The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signal of an individual from a transmitter of a mechanism with a sensor mechanism having a unique characteristic of a wearing mechanism worn by an individual, said mechanism for  
10 obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

15           The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signal of an individual from a transmitter of a mechanism with a sensor mechanism sensing an acoustic characteristic of a wearing mechanism worn by an individual, said  
20 mechanism for obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signal of an individual from a transmitter of a mechanism with a sensor mechanism sensing an electric and/or magnetic characteristic of a wearing mechanism worn by an individual, said mechanism for obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signature of an individual from a transmitter of a touchless mechanism, said touchless mechanism for obtaining the biometric signature of the individual remotely from the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signature of an individual from a transmitter of a touchless mechanism having a sensor mechanism with unique characteristics, said touchless mechanism for obtaining the biometric signature of the individual remotely from the individual.

Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

5           The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signature of an individual from a transmitter of a touchless mechanism having a sensor mechanism sensing an acoustic characteristic, said touchless mechanism for obtaining the  
10 biometric signature of the individual remotely from the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

15           The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signature of an individual from a transmitter of a touchless mechanism having a sensor mechanism sensing an electric and/or magnetic characteristic, said touchless mechanism for  
20 obtaining the biometric signature of the individual remotely from the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of obtaining a biometric signature of an individual with a biometric mechanism worn by the individual. Next there is the step of transmitting a  
5 unique ID of the biometric mechanism and the biometric signal obtained from the biometric mechanism of the individual wearing the biometric mechanism with a transmitter/receiver of the biometric mechanism. Next there is the step of receiving the unique ID and the biometric signal at a recognizing mechanism with a  
10 transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of an individual with the recognizing mechanism. Then there is the step of determining where the individual is located.

The present invention pertains to a method for  
15 monitoring. The method comprises the steps of obtaining a biometric signature of an individual with a biometric mechanism with a sensor mechanism having a unique characteristic worn by the individual. Next there is the step of transmitting a unique ID of the biometric mechanism and the biometric signal obtained from the  
20 biometric mechanism of the individual wearing the biometric mechanism with a transmitter/receiver of the biometric mechanism. Next there is the step of receiving the unique ID and the biometric signal at a recognizing mechanism with a transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing  
25 the biometric signature of an individual with the recognizing

mechanism. Then there is the step of determining where the individual is located.

5 The present invention pertains to a method for monitoring. The method comprises the steps of obtaining a biometric signature of an individual with a biometric mechanism worn with a sensor mechanism sensing an acoustic characteristic by the individual. Next there is the step of transmitting a unique ID of the biometric mechanism and the biometric signal obtained from the biometric mechanism of the individual wearing the biometric  
10 mechanism with a transmitter/receiver of the biometric mechanism. Next there is the step of receiving the unique ID and the biometric signal at a recognizing mechanism with a transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of an individual with the recognizing  
15 mechanism. Then there is the step of determining where the individual is located.

20 The present invention pertains to a method for monitoring. The method comprises the steps of obtaining a biometric signature of an individual with a biometric mechanism worn with a sensor mechanism sensing an electric and/or magnetic characteristic by the individual. Next there is the step of transmitting a unique ID of the biometric mechanism and the biometric signal obtained from the biometric mechanism of the individual wearing the biometric mechanism with a  
25 transmitter/receiver of the biometric mechanism. Next there is the



step of receiving the unique ID and the biometric signal at a recognizing mechanism with a transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of an individual with the recognizing  
5 mechanism. Then there is the step of determining where the individual is located.

The present invention pertains to a method for tracking. The method comprises the steps of obtaining a biometric signature of an individual. Next there is the step of sending information  
10 and the biometric signature of the individual with an individual transmitter/receiver to a recognizing transmitter/receiver of a recognizing mechanism for recognizing the individual. Next there is the step of receiving the information and the biometric signature of the individual with the transmitter/receiver of the  
15 recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual. Next there is the step of ascertaining the position of the individual from a GPS.

The present invention pertains to a method for tracking. The method comprises the steps of obtaining a biometric signature  
20 of an individual with a sensor mechanism having a unique characteristic. Next there is the step of sending information and the biometric signature of the individual with an individual transmitter/receiver to a recognizing transmitter/receiver of a recognizing mechanism for recognizing the individual. Next there  
25 is the step of receiving the information and the biometric

signature of the individual with the transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual. Next there is the step of ascertaining the position of the individual from a GPS.

5           The present invention pertains to a method for tracking. The method comprises the steps of obtaining a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of sending information and the biometric signature of the individual with an individual  
10 transmitter/receiver to a recognizing transmitter/receiver of a recognizing mechanism for recognizing the individual. Next there is the step of receiving the information and the biometric signature of the individual with the transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the  
15 biometric signature of the individual. Next there is the step of ascertaining the position of the individual from a GPS.

          The present invention pertains to a method for tracking. The method comprises the steps of obtaining a biometric signature of an individual with a sensor mechanism sensing an electric and/or  
20 magnetic characteristic of the individual. Next there is the step of sending information and the biometric signature of the individual with an individual transmitter/receiver to a recognizing transmitter/receiver of a recognizing mechanism for recognizing the individual. Next there is the step of receiving the information  
25 and the biometric signature of the individual with the

transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of ascertaining the  
5 position of the individual from a GPS.

The present invention pertains to a method for tracking. The method comprises the steps of recognizing the biometric signature of the individual. Next there is the step of ascertaining the position of the individual from a GPS when the  
10 biometric signature of the individual is recognized.

The present invention pertains to a method for tracking. The method comprises the steps of recognizing the biometric signature of the individual with a sensor mechanism having a unique characteristic. Next there is the step of ascertaining the  
15 position of the individual from a GPS when the biometric signature of the individual is recognized.

The present invention pertains to a method for tracking. The method comprises the steps of recognizing the biometric signature of the individual with a sensor mechanism sensing an  
20 acoustic characteristic. Next there is the step of ascertaining the position of the individual from a GPS when the biometric signature of the individual is recognized.

The present invention pertains to a method for tracking. The method comprises the steps of recognizing the biometric signature of the individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of  
5 ascertaining the position of the individual from a GPS when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of identifying  
10 an amount of cash to be distributed to the individual in a control unit. Then there is the step of distributing cash to the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing  
15 cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of identifying an amount of cash to be distributed to the individual in a control unit. Then there is the step of distributing cash to the individual when the  
20 biometric signature of the individual is recognized.

The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of identifying an

amount of cash to be distributed to the individual in a control unit. Then there is the step of distributing cash to the individual when the biometric signature of the individual is recognized.

5           The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of identifying an amount of cash to be distributed to the individual  
10 in a control unit. Then there is the step of distributing cash to the individual when the biometric signature of the individual is recognized.

          The present invention pertains to a method for authenticating an individual. The method comprises the steps of  
15 touching a sensor mechanism by the individual to generate a biometric signature of the individual. Next there is the step of placing the sensor mechanism in communication with a reader. Then there is the step of reading the sensor mechanism with the reader and recognizing the individual from the biometric signature.

20           The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism with a unique characteristic by the individual to generate a biometric signature of the individual. Next there is the step of placing the sensor mechanism in

communication with a reader. Then there is the step of reading the sensor mechanism with the reader and recognizing the individual from the biometric signature.

5 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism for sensing an acoustic characteristic by the individual to generate a biometric signature of the individual. Next there is the step of placing the sensor mechanism in communication with a reader. Then there is the step of reading  
10 the sensor mechanism with the reader and recognizing the individual from the biometric signature.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism for sensing an electric and/or magnetic  
15 characteristic by the individual to generate a biometric signature of the individual. Next there is the step of placing the sensor mechanism in communication with a reader. Then there is the step of reading the sensor mechanism with the reader and recognizing the individual from the biometric signature.

20 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism by the individual to generate a biometric signature of the individual. Then there is the step of reading the sensor mechanism to obtain the biometric signature of

the individual and a memory having known biometric signatures with a reader. Then there is the step of recognizing the individual from the biometric signature.

5 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism with a unique characteristic by the individual to generate a biometric signature of the individual. Then there is the step of reading the sensor mechanism to obtain the biometric signature of the individual and a memory having known  
10 biometric signatures with a reader. Then there is the step of recognizing the individual from the biometric signature.

15 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism for sensing an acoustic characteristic by the individual to generate a biometric signature of the individual. Then there is the step of reading the sensor mechanism to obtain the biometric signature of the individual and a memory having known biometric signatures with a reader. Then there is the step of recognizing the individual from the biometric signature.

20 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism for sensing an electric and/or magnetic characteristic by the individual to generate a biometric signature of the individual. Then there is the step of reading the sensor

mechanism to obtain the biometric signature of the individual and a memory having known biometric signatures with a reader. Then there is the step of recognizing the individual from the biometric signature.

5           The present invention pertains to a method for recognizing an individual. The method comprises the steps of sensing a biometric signature of the individual with a touchless sensor for a non-facial feature of the individual. Then there is the step of recognizing an individual.

10           The present invention pertains to a method for recognizing an individual. The method comprises the steps of recognizing a biometric signature of the individual with a touchless sensor having a unique characteristic for a non-facial feature of the individual. Then there is the step of allowing the  
15 action to occur.

          The present invention pertains to a method for recognizing an individual. The method comprises the steps of recognizing a biometric signature of the individual with a touchless sensor for sensing an acoustic characteristic for a non-  
20 facial feature of the individual. Then there is the step of allowing the action to occur.

          The present invention pertains to a method for recognizing an individual. The method comprises the steps of



recognizing a biometric signature of the individual with a touchless sensor for sensing an electric and/or magnetic characteristic for a non-facial feature of the individual. Then there is the step of allowing the action to occur.

5           The present invention pertains to a method for recognizing an individual. The method comprises the steps of flipping up a flip-up sensor for obtaining a biometric signature of an individual. Next there is the step of touching by the individual the sensor. Next there is the step of recognizing the  
10 biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

          The present invention pertains to a method for recognizing an individual. The method comprises the steps of flipping up a flip-up sensor having a unique characteristic for  
15 obtaining a biometric signature of an individual. Next there is the step of touching by the individual the sensor. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

20           The present invention pertains to a method for recognizing an individual. The method comprises the steps of flipping up a flip-up sensor for sensing an acoustic characteristic for obtaining a biometric signature of an individual. Next there is the step of touching by the individual the sensor. Next there

is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

5 The present invention pertains to a method for recognizing an individual. The method comprises the steps of flipping up a flip-up sensor for sensing an electric and/or magnetic characteristic for obtaining a biometric signature of an individual. Next there is the step of touching by the individual the sensor. Next there is the step of recognizing the biometric  
10 signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

15 The present invention pertains to a method for recognizing an individual. The method comprises the steps of touching by the individual a recessed sensor for obtaining a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

20 The present invention pertains to a method for recognizing an individual. The method comprises the steps of touching by the individual a recessed sensor having a unique characteristic for obtaining a biometric signature of an individual. Next there is the step of recognizing the biometric

signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

The present invention pertains to a method for recognizing an individual. The method comprises the steps of  
5 touching by the individual a recessed sensor for sensing an acoustic characteristic for obtaining a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

10 The present invention pertains to a method for recognizing an individual. The method comprises the steps of touching by the individual a recessed sensor for sensing an electric and/or magnetic characteristic for obtaining a biometric signature of an individual. Next there is the step of recognizing  
15 the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

The present invention pertains to a method for recognizing an individual. The method comprises the steps of sensing a biometric signature of an individual with a biometric PAN  
20 system having a sensor for obtaining the biometric signature of the individual. Then there is the step of recognizing the individual.

The present invention pertains to a method for recognizing an individual. The method comprises the steps of

recognizing a biometric signature of an individual with a biometric PAN system having a sensor with a unique characteristic for obtaining the biometric signature of the individual. Then there is the step of recognizing the individual.

5           The present invention pertains to a method for recognizing an individual. The method comprises the steps of recognizing a biometric signature of an individual with a biometric PAN system having a sensor for sensing an acoustic characteristic for obtaining the biometric signature of the individual. Then  
10 there is the step of recognizing the individual.

          The present invention pertains to a method for recognizing an individual. The method comprises the steps of recognizing a biometric signature of an individual with a biometric PAN system having a sensor for sensing an electric and/or  
15 magnetic characteristic for obtaining the biometric signature of the individual. Then there is the step of recognizing the individual.

          The present invention pertains to a method for recognizing an individual. The method comprises the steps of  
20 detecting a characteristic of an individual from energy emitted by the individual. Then there is the step of recognizing a biometric signature of the individual from the energy.

The present invention pertains to an apparatus for recognizing an individual. The apparatus comprises a mechanism for sensing a biometric signature of an individual from energy emitted by the individual. The apparatus comprises a mechanism for  
5 recognizing the individual.

The present invention pertains to an apparatus for accessing an area. The apparatus comprises a mechanism for determining a biometric signature of an individual. The apparatus  
10 comprises a door having a door handle in which sensors are disposed to obtain the biometric signature of the individual when the individual grabs or touches the handle. The apparatus comprises a reader for reading the biometric signature of the individual from the sensors. The reader is connected to the determining mechanism and the sensors. The apparatus comprises a memory having a known  
15 biometric signature of the individual. The determining mechanism connected to the memory and comparing the known biometric signature of the individual with the biometric signature of the individual obtained from the electrodes. The apparatus comprises a mechanism for unlocking the lock when the determining mechanism recognizes  
20 the biometric signature of the individual from the known biometric signature of the individual, said unlocking mechanism connected to the determining mechanism.

The present invention pertains to a method for accessing an area. The method comprises the steps of grabbing or touching by  
25 an individual a door handle of a door in which sensors are disposed

to obtain the biometric signature of the individual. Then there is the step of reading the biometric signature of the individual from the sensors. Next there is the step of comparing a known biometric signature of the individual with the biometric signature of the individual obtained from the sensors. Then there is the step of unlocking a lock of the door when the biometric signature of the individual from the known biometric signature of the individual is recognized.

#### BRIEF DESCRIPTION OF THE DRAWINGS

10 In order that the invention may readily be carried into practice, one embodiment will now be described in detail, by way of non-limiting example only, with reference to the accompanying drawings in which:

15 Figure 1 comprises a block diagram illustrating one preferred embodiment of the present invention.

Figure 2 is a block diagram illustrating a periodic controller connected to a current generator.

Figure 3 is a pictorial representation of a hand attached to a biometric system of the present invention.

20 Figure 4 is a representative graph of voltage measurement values plotted against multi-frequencies.

Figures 5a-5f are charts of subjects regarding impedance and digits.

Figures 6a-6f are charts of subjects regarding impedance and digits.

5           Figures 7 and 8 show alternative embodiments illustrating the biometric recognition system utilized in a keyboard and mouse.

Figure 9 is an illustration showing the biometric recognition system of the present invention incorporated into the handpiece of a firearm.

10           Figure 10 is an illustration showing the biometric recognition system incorporated into a wrist watchband.

Figure 11 is a flow chart of a method of the invention.

15           Figures 12a and 12b are side and overhead views of a non-contact apparatus for the interruption of an electric field of the present invention.

Figure 13 is a schematic representation of an apparatus for sensing electric or magnetic properties of an organism.

Figure 14 is a schematic representation of an apparatus for sensing the magnetic properties of an organism.

Figure 15 is a schematic representation of an apparatus for inducing current longwise in an organism.

Figure 16 is a schematic representation of the flow of induced current from the heel of the palm lengthwise to the finger tips.

Figure 17 is a schematic representation of an apparatus for the measurement of induced current in regard to a stationary hand.

Figure 18 is a schematic representation of an apparatus for the measurement of induced current in regard to a moving hand.

Figure 19 is a schematic representation of an apparatus for inducing current in an organism using an electromagnetic field.

Figure 20 is alternative embodiment of an apparatus for inducing current in an organism with an electric and/or magnetic field.

Figure 21 is a schematic representation of an apparatus for sensing the interruption of an electromagnetic field.

Figure 22 is a schematic representation of sensing electric and/or magnetic properties based upon reflection of electromagnetic radiation from an organism.



Figure 23 is a schematic representation of an apparatus for measuring the interruption of an electromagnetic field by measuring only the electric field.

Figures 24-33 are circuit diagrams for an apparatus for  
5 sensing electric or magnetic properties of a hand piece or mouse or keyboard.

Figure 34 is a schematic representation of a side view of a hand unit.

Figure 35 is a schematic representation of an overhead  
10 view of a hand unit.

Figure 36 is a schematic representation of a keyboard having electrodes.

Figure 37 is a schematic representation of a hand grasping a mouse having electrodes.

15 Figure 38 is a schematic representation of a mouse having electrodes.

Figure 39 is a side view of a wrist band having electrodes.

Figure 40 is a schematic representation of electrode placement and current path of measurement from the palm to the thumb.

Figure 41 is a two-dimensional impedance plot  
5 corresponding to the electrode placement of figure 40.

Figure 42 is a schematic representation of measurement sites for back to front capacitive plate measurements from the palm to the thumb.

Figure 43 is a two dimensional impedance plot regarding  
10 resistance at a single frequency corresponding to the measurement sites of figure 42.

Figure 44 is a schematic representation of measurement sites from the palm to each finger-tip.

Figure 45 is a three-dimensional plot at a single  
15 frequency regarding measurements from the measurement sites of figure 44.

Figure 46 is a four-dimensional plot at four different frequencies from the palm to each finger-tip.

Figure 47 is a schematic representation of electrodes for  
20 one finger.

Figure 48 is a three-dimensional plot at a single frequency from electrode to electrode for one finger as shown in figure 47.

Figure 49 is a four-dimensional plot at a single  
5 frequency from electrode to electrode for each finger.

Figure 50 is a schematic representation of an acoustic beam at a single frequency passing through the thumb from the side of the thumb.

Figure 51 is a two-dimensional acoustic plot at a single  
10 frequency regarding figure 50 where the plot is of amplitude versus time.

Figure 52 is a schematic representation of acoustic energy at a single frequency passing through the side, center and other side of the thumb by varying the location of the thumb  
15 relative to the acoustic energy.

Figure 53 is a three-dimensional plot regarding figure 52.

Figure 54 is a four-dimensional plot at four different frequencies through the side, center and other side of the thumb.

Figure 55 is a five-dimensional plot with sine, square and ramped waveforms at four different frequencies through the side, center and other side of the thumb.

Figure 56 is a five-dimensional plot at three different  
5 frequencies from electrode to electrode for each finger.

Figure 57 is a six-dimensional plot with sine, ramped and square wave forms at three different frequencies from electrode to electrode for each finger.

Figure 58 is a five-dimensional plot with sine, square  
10 and ramped waveforms at four different frequencies from the palm to each finger-tip.

Figure 59 is a picture of a bone with an arrow representing normal current in a bone.

Figure 60 is a picture of a bone having a fracture or  
15 break with current interrupted due to the fracture or break.

Figure 61 is a schematic representation of a galvanometer at 0 current reading relative to a bone having a fracture or break where the current has been induced by an apparatus which induces current in a bone.

Figure 62 is a schematic representation of a galvanometer showing normal current in a healthy bone where the current has been induced by an apparatus which induces current in a bone.

Figure 63 is a drawing of a 1 cm and 1.25 cm diameter  
5 electrode.

Figure 64 is a schematic representation of a cross-sectional enlarged view of an electrode.

Figure 65 is a side view of an electrode.

Figure 66 shows a flip-up sensor.

10 Figure 67 shows an acoustic mechanism for generation of direct current.

Figure 68 shows an acoustic apparatus for the generation of alternating current and magnetic fields.

Figure 69 shows an apparatus for detection of direct  
15 current or alternating current induced by acoustic energy.

Figure 70 shows an apparatus for the detection of alternating current induced by acoustic energy.

Figure 71 shows an apparatus which produces an acoustic wave by electric and/or magnetic energy.

Figure 72 is a schematic representation of an apparatus for charging a purchase.

5           Figure 73 is a schematic representation of a card and a reader.

Figure 74 is a schematic representation of an alternative apparatus for charging a purchase.

10           Figure 74a is a schematic representation of a smart card and reader of an acoustic biometric system.

Figure 75 is a schematic representation of a first side of a contact card with bar code.

Figure 75a is a schematic representation of the front of an acoustic smart card.

15           Figure 75b is a schematic representation of the back of an acoustic smart card.

Figure 76 is a schematic representation of a second side of a touch contact card with bar code.

Figure 77 is a schematic representation of a top view of a reader for a contact card with bar code.

Figure 77a is a schematic representation of a card and reader of an acoustic biometric system.

5           Figure 78 is a schematic representation of a side view of a reader groove for a contact card with bar code.

Figure 78a is a schematic representation of a contactless acoustic smart card and reader of an acoustic biometric system.

10           Figure 79 is a schematic representation of a contact card and a reader for a contact card with memory.

Figure 79a is a schematic representation of the front of an electrode smart card.

Figure 79b is a schematic representation of the back of an electrode smart card.

15           Figure 80 is a schematic representation of a first side of a contact card with magnetic strip.

Figure 81 is a schematic representation of a second side of a contact card with magnetic strip.

Figure 82 is a schematic representation of a first side of a contact card with sensors.

Figure 83 is a schematic representation of a second side of a contact card with sensors.

5           Figure 84 is a schematic representation of a contact card with embedded microchip and a reader for a contact card with embedded microchip.

10           Figure 85 is a schematic representation of a contact card with microprocessor and a reader for a contact card with microprocessor.

Figure 86 is a schematic representation of a first side of a contact card with bar code and magnetic strip.

Figure 87 is a schematic representation of a second side of a contact card with bar code and magnetic strip.

15           Figure 88 is a schematic representation of a first side of a contactless card.

Figure 89 is a schematic representation of a second side of a contactless card.



Figure 90 is a schematic representation of a contactless card and a reader for a contactless card.

Figure 91 is a schematic representation of an apparatus for charging a purchase.

5           Figure 92 is a schematic representation of an apparatus for authorizing an action.

Figure 92a is a schematic representation of an authorizing action schematic.

10           Figure 93 is a schematic representation of an alternative embodiment of an apparatus for authorizing an action.

Figure 94 is a schematic representation of the sensor and reader in the same housing.

Figure 95 is a schematic representation of the sensor and reader in separate housing.

15           Figure 96 is a schematic representation of the reader and determining mechanism in the same housing.

Figure 97 is a schematic representation of the reader and determining mechanism in separate housing.

Figure 98 is a schematic representation of the memory and sensor in the same housing.

Figure 99 is a schematic representation of the memory and reader in the same housing.

5           Figure 100 is a schematic representation of the memory and determining mechanism in the same housing.

Figure 101 is a schematic representation of memory in separate housing.

10           Figure 102 is a schematic representation of the sensor, reader and determining mechanism in the same housing.

Figure 103 is a schematic representation of the sensor, reader and memory in the same housing.

Figure 104 is a schematic representation of the reader, determining mechanism and memory in the same housing.

15           Figure 105 is a schematic representation of the sensor, reader, determining mechanism and memory in the same housing.

Figure 106 is a schematic representation of the sensor, determining mechanism and memory in the same housing.

Figure 107 is a schematic representation of the determining mechanism and action mechanism in the same housing.

Figure 108 is a schematic representation of the determining mechanism and action mechanism in separate housing.

5           Figure 109 is a schematic representation of ATM with hand piece and memory.

Figure 110 is a schematic representation of ATM with hand piece and memory by modem.

10           Figure 111 is a schematic representation of ATM with hand piece; pattern data communicated to bank computer for comparison.

Figure 112 is a schematic representation of teller hand piece; pattern data and known pattern memory communicated to teller computer for comparison.

15           Figure 113 is a schematic representation of teller hand piece; pattern data communicated to teller computer for comparison.

Figure 114 is a schematic representation of a bank card with acoustic sensor.

Figure 115 is a schematic representation of a home computer with keyboard electrodes.

Figure 116 is a schematic representation of kiosk with touchless C-arm electric sensor.

Figure 117 is a schematic representation of a casino electrode card with memory in casino computer.

5           Figure 118 is a schematic representation of a casino electrode card with memory in card.

Figure 119 is a schematic representation of a casino electrode card with memory with reader.

10           Figure 120 is a schematic representation of a casino sensor/reader with present pattern memory in determining unit.

Figure 121 is a schematic representation of a home computer with acoustic transducer mouse.

Figure 122 is a schematic representation of a casino room door handle.

15           Figure 123 is a schematic representation of wristbands for video arcade.

Figure 124 is a schematic representation of a utility box.

Figure 124a is a representation of a utility box.

Figure 125 is a schematic representation of a homeowner's electric meter with sensor card reader.

Figure 126 is a schematic representation of a homeowner's electric meter with touchless magnetic sweep hand sensors.

Figure 127 is a schematic representation for a subway commuter with hand piece; pattern data communicated to subway computer for comparison.

Figure 128 is a schematic representation for a turnpike commuter with acoustic biometric and infrared transmitter.

Figure 129 is a schematic representation for a bus rider with electrode stored value smart card.

Figure 130 is a schematic representation of a payphone for sensor/memory card.

Figure 131 is a schematic representation of an electrode payphone.

Figure 131a is a schematic representation of a side view of an electrode payphone.

Figure 131b is a schematic representation of a rear view of an electrode payphone.

Figure 132 is a schematic representation of a touchless microwave payphone.

5           Figure 132a is a schematic representation of a touchless microwave payphone.

Figure 133 is a schematic representation of an electronic payment authorization.

10           Figure 134 is a schematic representation of an MSA electrode card and reader.

Figure 135 is a schematic representation of an MSA smart card storing account and biometric information and a reader.

Figure 136 is a schematic representation of a portable electrode telephone.

15           Figure 137 is a schematic representation of a portable video phone with flip-up electrode sensor.

Figure 138 is a schematic representation of a television lock-out hand piece unit.

Figure 138a is a schematic representation of a television having a biometric lock.

Figure 138b is a schematic representation of a radio having a biometric lock.

5           Figure 139 is a schematic representation of a pay-TV electrode card.

Figure 140 is a schematic representation of a pay-TV touchless electric field sensor/reader and contact card with memory.

10           Figure 141 is a schematic representation of an airline check-in hand unit.

Figure 142 is a schematic representation of an airline remote check-in hand unit.

15           Figure 143 is a schematic representation of an airline touchless check-in hand unit and memory stick.

Figure 144 is a schematic representation of an airline touchless remote check-in hand unit with memory stick.

Figure 145 is a schematic representation of a customs electronic/sensor passport unit.

Figure 146 is a schematic representation of a customs touchless and contactless electronic passport.

Figure 147 is a schematic representation of a brokerage wireless PC transaction.

5           Figure 148 is a schematic representation of a brokerage wireless PC transaction.

Figure 148a is a schematic representation of a sensor unit in a lap-top computer.

10           Figure 148b is a schematic representation of an enlarged view of the sensor unit in a lap-top computer.

Figure 148c is a schematic representation of a side view of the sensor unit in a lap-top computer.

Figure 149 is a schematic representation of a retail electrode card for redeemable points.

15           Figure 150 is a schematic representation of a retail electrode card for redeemable points.

Figure 151 is a schematic representation of a retail touchless sensor for redeeming points.



Figure 152 is a schematic representation of a smart card driver's license.

Figure 153 is a schematic representation of a smart card passport.

5           Figure 154 is a schematic representation of a CIA computer room access.

Figure 155 is a schematic representation of a security room access.

10           Figure 156 is a schematic representation of a sensor smart identification card.

Figure 157 is a schematic representation of employee access monitoring and time tracking.

Figure 158 is a schematic representation of an electronic medical record notepad.

15           Figure 158a is a schematic representation of an electronic medical record notepad.

Figure 158b is a schematic representation of an electronic medical record notepad.

Figure 159 is a schematic representation of a smart sensor wristband.

Figure 160 is a schematic representation of a social services card.

5           Figure 161 is a schematic representation of a biometric glove.

Figure 161a is a schematic representation of a biometric glove.

10           Figure 161b is a schematic representation of a biometric glove.

Figure 162 is a schematic representation of software licensing.

Figure 162a is a schematic representation of a mouse.

Figure 162b is a schematic representation of a mouse.

15           Figure 162c is a schematic representation of a side view of the mouse button raised.

Figure 163 is a schematic representation of a discrete biometric lock.

Figure 163a is a schematic representation of a door handle with electrode sensor.

Figure 163b is a schematic representation of a door handle with electrode sensor.

5           Figure 163c is a schematic representation of a door handle with electrode sensor.

Figure 163d is a schematic representation of a door handle with electrode sensor.

10           Figure 163e is a schematic representation of a door handle with acoustic sensor.

Figure 163f is a schematic representation of a door handle with acoustic sensor.

Figure 163g is a schematic representation of a door handle with acoustic sensor.

15           Figure 163h is a schematic representation of a door handle with acoustic sensor.

Figure 164 is a schematic representation of a composite biometric lock.

Figure 165 is a schematic representation of a multiple biometric lock.

Figure 166 is a schematic representation of an optional composite biometric lock.

5           Figure 167 is a schematic representation of an optional multiple biometric lock.

Figure 168 is a schematic representation of a composite multiple biometric lock.

10           Figure 169 is a schematic representation of a closed laboratory access.

Figure 170 is a schematic representation of a biometric door access recording device.

Figure 170a is a schematic representation of a door handle electrode.

15           Figure 171 is a schematic representation of a restricted access database.

Figure 171a is a schematic representation of a restricted access database having a shell hand piece.



$10^{10}$   $10^{11}$   $10^{12}$   $10^{13}$   $10^{14}$   $10^{15}$   $10^{16}$   $10^{17}$   $10^{18}$   $10^{19}$   $10^{20}$   $10^{21}$   $10^{22}$   $10^{23}$   $10^{24}$   $10^{25}$   $10^{26}$   $10^{27}$   $10^{28}$   $10^{29}$   $10^{30}$   $10^{31}$   $10^{32}$   $10^{33}$   $10^{34}$   $10^{35}$   $10^{36}$   $10^{37}$   $10^{38}$   $10^{39}$   $10^{40}$   $10^{41}$   $10^{42}$   $10^{43}$   $10^{44}$   $10^{45}$   $10^{46}$   $10^{47}$   $10^{48}$   $10^{49}$   $10^{50}$   $10^{51}$   $10^{52}$   $10^{53}$   $10^{54}$   $10^{55}$   $10^{56}$   $10^{57}$   $10^{58}$   $10^{59}$   $10^{60}$   $10^{61}$   $10^{62}$   $10^{63}$   $10^{64}$   $10^{65}$   $10^{66}$   $10^{67}$   $10^{68}$   $10^{69}$   $10^{70}$   $10^{71}$   $10^{72}$   $10^{73}$   $10^{74}$   $10^{75}$   $10^{76}$   $10^{77}$   $10^{78}$   $10^{79}$   $10^{80}$   $10^{81}$   $10^{82}$   $10^{83}$   $10^{84}$   $10^{85}$   $10^{86}$   $10^{87}$   $10^{88}$   $10^{89}$   $10^{90}$   $10^{91}$   $10^{92}$   $10^{93}$   $10^{94}$   $10^{95}$   $10^{96}$   $10^{97}$   $10^{98}$   $10^{99}$   $10^{100}$

10

10

10

15

15

15

Figure 177b is a schematic representation of sensor virtual screen glasses.

Figure 178 is a schematic representation of access to computer hardware.

Figure 178a is a schematic representation of a scalloped electrode card.

5           Figure 179 is a schematic representation of a portable TV or radio.

Figure 180 is a schematic representation of an internal ATM hardware access.

10           Figure 181 is a schematic representation of a vehicle steering wheel biometric.

Figure 182 is a schematic representation of a biometric vehicle door access device.

Figure 182a is a schematic representation of a biometric vehicle steering wheel.

15           Figure 182b is a schematic representation of a biometric vehicle steering wheel.

Figure 183 is a schematic representation of a vehicle sensor key.

Figure 183a is a schematic representation of a vehicle sensor key.

Figure 183b is a schematic representation of a vehicle sensor key reader.

5           Figure 184 is a schematic representation of an ankleband house arrest.

Figure 185 is a schematic representation of a ship's locator system.

10           Figure 185a is a schematic representation of a contactless acoustic band.

Figure 185b is a schematic representation of an outside view of a contactless acoustic band.

Figure 185c is a schematic representation of an inside view of a contactless acoustic band.

15           Figure 185d is a schematic representation of a contactless electrode watch.

Figure 185e is a schematic representation of an outside view of a contactless electrode watch.

Figure 185f is a schematic representation of an inside view of a contactless electrode watch.

Figure 186 is a schematic representation of a GPS locator/verification system.

5           Figure 187 is a schematic representation of a remote control biometric system.

Figure 188 is a schematic representation of an MSA transducer card reader.

10           Figure 189 is a schematic representation of a portable video phone with molded transducer.

Figure 190 is a schematic representation of a pay-TV transducer card reader.

Figure 191 is a schematic representation of an acoustic hand piece at a cash register.

15           Figure 192 is a schematic representation of a driver's license reader computer.

Figure 193 is a schematic representation of a smart card reader.



Figure 194 is a schematic representation of a mouse sensor.

Figure 195 is a schematic representation of a card ATM reader-ATM computer.

5           Figure 196 is a schematic representation of a card-wireless car system.

Figure 197 is a schematic representation of an ankleband-sensor.

10           Figure 198 is a schematic representation of an electric circuit for a hand piece.

Figure 199 is a schematic representation of a circuit for a hand unit.

15           Figure 200 is a schematic representation of a block diagram of an alternative embodiment of an apparatus for authorizing an action.

Figure 201 is a schematic representation of a block diagram of a discrete biometric lock system.

Figure 202 is a schematic representation of a block diagram of a composite biometric lock system.

Figure 203 is a schematic representation of a block diagram of a multiple biometric lock system.

Figure 204 is a schematic representation of a block diagram of a composite multiple biometric lock system.

5           Figure 205 is a schematic representation of a block diagram of an optional multiple biometric lock system.

Figure 206 is a schematic representation of a block diagram of an optional composite biometric lock system.

10           Figure 207 is a schematic representation of a block diagram of another alternative embodiment of an apparatus for authorizing an action.

#### DESCRIPTION OF THE PREFERRED EMBODIMENT

15           The preferred embodiments of the present invention and their advantages are best understood by referring to figures 1-11 of the drawings, like numerals being used for like and corresponding parts of the various drawings.

20           Before explaining the present invention in its best mode, a general explanation of electrical and magnetic properties will help to provide a better understanding of the invention. For purposes herein the term "field" herein includes but is not limited

to waves, current, flux, resistance, potential, radiation or any physical phenomena including those obtainable or derivable from the Maxwell equations, incorporated by reference herein.

5 The electrical conductivity of a body segment depends  
upon a number of factors including the length and cross-sectional  
area of a segment of tissue and the composition of tissue including  
lean and fatty tissue. There may be day to day variations in  
conductivity and other electrical measurements due to body weight  
adjustments and changes in body fluids and electrolyte composition  
10 but the changes are fairly consistent through the different body  
segments being analyzed because of the systemic physical  
characteristics of each organism. For instance, it is well known  
in regard to clinical impedance measurements that the impedance  
variations in a subject due to physiological changes, are smaller  
15 than the variability among normal subjects. See "CRC Handbook of  
Biological Effects of Electromagnetic Fields", generally and  
specifically pages 8, 9 and 76, incorporated by reference herein.

When measuring electrical and/or magnetic properties of  
an individual for biometric recognition purposes whether applying  
20 energy by the contact method or by the non-contact method, several  
different measurements may be utilized such as, impedance,  
resistance, reactance, phase angle; current, or voltage  
differential, across a measured body segment. For instance,  
impedance is a function of two components, that being the  
25 resistance of the tissue to the flow of current and reactance which

is additional opposition to the current due to capacitant effect of membranes, tissue interfaces, and other biocapacitant tissue.

Many bioimpedance measurements in the prior art depend on the assumption that the relationship of body composition such as  
5 body fluid and tissue mass is dynamic, and that fluctuations occur. As fluids increase in the tissue, the bioimpedance signal decreases in value because the segment being measured has an increase in conductive potential due to the increase in fluid volume. Increases in segmental fluid volume will decrease  
10 bioimpedance values. Decreases in segmental fluid will decrease the conductive potential and thus increase the bioimpedance value. However, it is known for the operation of the present invention that the daily fluctuation is consistent systemically through the body and the overall ratio between impedance values taken from  
15 different segments of a body part will remain constant.

Referring now to the drawings, figure 1 describes a preferred embodiment utilizing an electrical current applied directly to the body part of a testing individual through surface contacting electrodes for generating a biometric pattern of the  
20 testing organism. Biometric recognition system 10 is a device wherein the electric and/or magnetic properties of a body segment is measured by applying an input electrical signal in the form of a constant magnitude current to the body segment tissue and measuring the resulting voltage. Since  $R=V/I$ , the measured voltage

yields either a relative or calculated resistance. The voltage or resistance pattern is unique for an individual.

It is also contemplated in the present invention that a constant magnitude voltage signal is applied to the tissue and the  
5 resulting current is used to determine the bioelectrical characteristics of the testing segment.

For purposes of description, the contact system of the present invention described below uses a constant magnitude alternating current source, but direct current may be used  
10 especially in some devices that may require the introduction of an internal battery for a power source. In the event direct current is used in the contact system, an oscillator may be used to convert the direct current to an alternating current. The system 10 comprises a current generator 12 which is connected to excitation  
15 electrodes 14, 16 positioned on a body part of a testing individual, such as a hand shown in figures 1 and 3. System 10 further comprises an analyzer 22 which is connected and receives an output voltage signal from receiver electrodes 18 and 20. The analyzer 22 receives the voltage output signal which is produced  
20 between electrodes caused by a flow of current between electrodes 18 and 20 in response to the current flowing from current generator 12. The current generator comprises a current source for generating a constant magnitude current. The identification system of the present invention may utilize a continuous, constant  
25 magnitude current or periodic, constant magnitude current.

Periodic signals may include sinusoidal, square wave, ramp and sawtooth. Generally, the constant current magnitude ranges from about 1 microamp to 4 milliamps. Typically, the signal frequency may be between about 40 Hz to about 400 MHZ which is a frequency magnitude range within accepted risk standards for electrically susceptible humans. The present invention may utilize a single, predetermined frequency or multiple, variable frequencies within the above disclosed range. It should be noted that any frequency other than that described above may also be used in the present invention as long as electrical and/or magnetic properties of the tissue can be measured accurately. A disadvantage to using frequencies below 40 Hz can be that the measurements take longer and longer fractions of a second to complete. This can lengthen the overall time required to obtain a biometric pattern.

Each different frequency applied in the system has a different effect in the body segment due to membrane physiology, and tissue structure and composition, with accompanying changes in capacitance and inductance. When using multiple frequencies during the testing mode the output signals provide a unique biometric measurement pattern that is predictive of the individual being tested. The same is also true for changing waveform, angular frequency, capacitance and inductance at a singular frequency, as additional examples.

If a periodic, constant magnitude current is preferred, current generator 12 may be connected to a controller 24 which is

capable of generating periodic output signal to control the current generator as shown in figure 2. Bioimpedance measurement systems using a periodic constant current are well known in the art and described in U.S. Pat. No. 5,503,157, the disclosure of which is  
5 incorporated by reference herein.

The output signal of the current generator, is transmitted to excitation electrodes 14 and 16 through connectors 15 and 13 respectively. For purposes of illustration, figure 1 shows a tetrapolar electrode placement in which two of the  
10 electrodes are active for injecting the current while two electrodes are passive for detecting the resultant signal. It is contemplated that a bipolar setup or two electrodes may be utilized in the present invention especially in systems having minimum surface area for placement of electrodes.

15 In the tetrapolar electrode system the first excitation electrode 14 may be positioned on the palm heel of the hand while the second excitation electrode 16 is positioned on the palmar tip of the thumb. Similar electrode pairs may be placed and spaced a sufficient distance from each other to provide a drop in voltage on  
20 the remaining four digits so that the hand will have at least five distinct segments to be tested. This is by way of example only since other electrode configurations may also be used with the present method.

The present invention prefers the tetrapolar setup of electrodes to overcome the inconsistency that may occur in the impedance measurement values due to external contact resistance. External resistance may change significantly with certain specific changes such as those due to skin moisture. As such, this can be improved by using a tetrapolar system. The tetrapolar electrode system is superior to other electrode systems in that it eliminates both electrode polarization and also contact resistance effects between the electrodes and the body part being measured. Contact resistance is variable with the motion of the subject and creates motion artifacts which interfere with measurement of electrical parameters of the body. By applying the current to the subject through one pair of electrodes and measuring voltage differences through another pair of electrodes, the contact resistance and the inherent voltage drop is eliminated from the voltage measurement. The path the energy takes is not critical, except that it should approximate the path taken for obtaining the reference pattern.

It should be understood that in some systems of the present invention, the injection of current and the sensing of the voltage may be accomplished with two electrodes for the bioelectric measurements. However, as stated earlier, with the bipolar setup the measured voltages are the voltage drops along the current pathway which include both the internal impedance and the boundary contact impedance. The voltage drop across the contact impedance can be significant compared with the voltage drop across the internal impedance. To overcome this problem when using a two-



electrode system a compound electrode may be used. A compound electrode is a single electrode that incorporates an outer electrode to inject the current and an inner electrode to measure the voltage. A suitable compound electrode, for example, is disclosed by Ping Hua, 1993, Electrical Impedance Tomography, *IEEE Trans. Biomed. Eng.*, Jan. 40 (1), 29-34, which is incorporated herein by reference in its entirety. It should be noted that tetrapolar or compound electrodes are not necessary because switching can be used so that transmission and reception from the same electrode does not occur at the same time.

A variety of electrodes are commercially available and well known in the art such that structure and application will not be described in detail. Typically, any type of electrode known in the art that conducts an electrical signal may be used in the present invention. Of particular utility are the current synthetic conductive polymers, including polyacetylene, polypyrrole, poly-3,4-ethylene dioxythiophene, conductive adhesive polymers, semiconducting polymers, conductive silicone rubbers, and conductive rubbers all of which may be used to fabricate conductive inserts in a biometric recognition system such as shown in figures 7-10.

Unit 11, shown in figure 1, provides a surface for placing the measured body part, such as a hand. This unit may be constructed so that the conductive electrodes are mounted on the flat surface of the holder for contact with the fingers, thumb and

the palm heel. It should be understood that Unit 11 is only one embodiment envisioned by the inventor.

Since the bioelectrical measurements that are used to recognize an individual include the application or generation of current in the subject, the question of safety arises. As such, the biometric system of the present invention may further introduce the use of a transformer between the signal source generator and contacting electrodes thereby isolating the individual from potential electrical hazard. Any transformer that will transmit the required frequency associated with the constant current but will not conduct 300 cycles and preferably 60 cycles or higher of voltage in current may be utilized in this system.

Impedance to the current flow in the body segment generates a voltage difference across the body segment. The amplitude of the voltage is modulated by changes in the body segment's electrical conductivity caused by differences in tissues and structures. Receiving electrodes 18 and 20, positioned between the excitation electrodes, in this embodiment, are used to measure the voltage difference produced by the injected current through the measured segment of the body part. The receiving electrodes are generally the same types as that used for excitation electrodes. A voltage signal proportional to the body segments' impedance is generated within the body segment and the voltage difference measured between electrode 18 and 20 is an alternating voltage produced in response to the constant magnitude alternating current.

The voltage detector 28 may be any type well known to designers of electronic circuitry such as a voltmeter, potentiometer and the like.

5 Voltage detector 28 can be of the type that detects the magnitude of the voltage signal and also detects the phase relation between the alternating voltage and the alternating current producing the voltage. Therefore, both the resistive and reactive components of impedance may be measured. This type of detector is well known to electrical designers and often termed synchronous  
10 detectors. Impedance measuring systems utilizing synchronous detectors are described in U.S. Pat. Nos. 3,871,359 and 5,063,937, the contents of which are incorporated by reference herein.

Before the voltage signal is received by the voltage detector 28 and depending on the strength of the signal, an  
15 amplifier 26 may be connected between the signal received from the receiver electrodes 18 and 20 and the voltage detector. The amplifiers which can be advantageously used in the present invention are well known and widely used in electronic circuitry art. A suitable amplifier to be used in the present invention will  
20 take a signal less than a millivolt and amplify it to volts, will produce a large voltage gain without significantly altering the shape or frequencies present, and provide accurate measurements.

It is further contemplated in the present invention to provide a means to eliminate noise from the signal. As such, a

differential amplifier may be used in the present invention to remove background noise. If a differential amplifier is used another electrode will need to be added to the bioimpedance system to serve as a common ground.

5           Once the voltage signal is measured, the signal may be directed through an analog to digital converter 30 and the digital signal is directed into a microprocessor 32 which can automatically and instantaneously calculate impedance or any of the other bioelectrical characteristics of the body segment. Any general  
10   purpose computer or one capable of performing various mathematical operations on the voltage input information may be used in the present invention. A typical mathematical operation contemplated on the signal within the scope of this invention is the division of one impedance value by a subsequent detected impedance value from  
15   a second segment of a body part to compute a comparative ratio. The computation of a representative bioimpedance measurement pattern is illustrated by referring to figure 3. The voltage difference in each of five different segments that being A, B, C, D, and E are detected and subsequently a comparative ratio is  
20   determined by dividing one signal detected by a subsequent detected value. As an example  $A/A$ ,  $B/A$ ,  $C/A$ ,  $D/A$  and  $E/A$  are computed and the resultant values give four comparative ratios for the body part for a predetermined frequency. This yields a ratio of each finger to the thumb, for instance. Then when measurements are taken on  
25   another day, even though the absolute measurements will vary, the ratios are still the same(to within 0-6%). If the frequency is

then changed, another set of comparative ratios may be determined for the same body part. The more frequencies applied the larger the set of comparative ratios which may be used as a unique representative bioimpedance measurement pattern. Figure 4 shows a set of the comparative ratios identified above, with series 1 (the thumb) set to 10. The frequencies measured were in Hz (on the horizontal axis 1-15):

	10
	20
10	50
	100
	200
	500
	1,000
15	2,000
	5,000
	10,000
	20,000
	50,000
20	100,000
	200,000
	500,000.

Frequency #10 (10,000 Hz) is an impedance resonance point for the thumb, while the fingers have resonance points around 50,000 Hz.

Figures 5a-5f are charts of subjects showing impedance versus the fingers of the same subjects at different frequencies. Figures 6a-6f are charts of subjects showing impedance versus the fingers of several subjects at the same frequency.

5 Another operation contemplated is the computation of impedance values or any of the other bioelectrical and/or magnetic characteristics for each segment for a plurality of frequencies. The results of these values plotted against the range of multi-frequencies will provide a representative bioelectric measurement  
10 pattern in the form of a unique curve for each body segment, for example figure 4 shows a plot for segments A-E of figure 3 over a range of multi-frequencies.

The results of the computations are compared with a previously stored reference pattern stored in memory 36 to  
15 determine a match within an acceptable error range.

The results from the comparison are displayed on display unit 34 which may be a digital display component of the microprocessor.

20 While the present invention has been described using the flat hand detector, it should be appreciated that other embodiments of the described system and its elements may be used in other devices to gain access to or activate certain secure systems. For example, figures 7, 8, 9, and 10 illustrate just a few of the

contemplated setups and uses for the biometric recognition utilizing unique electrical conductivity values of an individual.

Figure 7 illustrates a computer keyboard having electrodes imbedded in specific keys for generating bioelectrical conductivity values. If the user's bioelectrical pattern matches that of an authorized individual the computer is activated and the person is allowed to log on.

Figure 8 illustrates another embodiment for access to a secure system using the mouse of a microprocessor. This system will recognize authorized users and prevent others from gaining access to the system.

Figure 9 provides a system to limit the use of a weapon such as a firearm to only the authorized user. If an unauthorized individual attempts to discharged the weapon, the system will not recognize the individual thereby preventing the activation of the firing mechanism.

Figure 10 provides for a simple recognition system that merely provides an individual's biometric characteristic pattern. The measurement electrodes are contained within the watchband wherein conductivity and/or other electrical values are measured in the wrist of an individual. An auxiliary receiving system recognizes the pattern sent from the watch and verifies the identity of the user. This watch, emitting an unique pattern may

be used to open an electronic door lock and replaces the need for a keypad or a remote control unit. Figure 11 is a flow chart of a method of the invention.

Referring to figures 12,13 and 14, the present invention  
5 pertains to an apparatus 100 for recognition of an individual living organism's identity. The apparatus 100 comprises a sensing mechanism 101 for sensing electric and/or magnetic properties of the organism. The apparatus 100 comprises a mechanism 102 for recognizing the organism. The recognizing mechanism 102 is in  
10 communication with the sensing mechanism 101.

Preferably, the recognizing mechanism includes a microprocessor 103 having a known electric and/or magnetic property of the individual organism. The sensing mechanism 101 preferably includes a mechanism 104 for producing an electric field and/or  
15 magnetic field in the organism, and a mechanism 105 for receiving the electric field and/or magnetic field. Preferably, the producing mechanism includes a frequency generator 106 and an electric field transmitter 107 and/or magnetic field transmitter 107 transmitter connected to the frequency generator 106, and the  
20 receiving mechanism 105 includes an electric field receiver 108 and/or magnetic field receiver 108 disposed adjacent to the electric field transmitter 107 or magnetic field transmitter and defining a test zone 110 with the electric field or magnetic field in which a portion of the individual organism is placed for sensing  
25 the electric or magnetic properties of the individual organism, and



a detector 111 connected to the electric field or magnetic field receiver 108 and the microprocessor 103. The detector mechanism preferably measures phase or amplitude or frequency or waveform of the electric field or magnetic field or acoustic field which extends through the test zone received by the receiver. The apparatus 100 can include a housing 112, and the transmitter and receiver are disposed in the housing. See also U.S. Patent 4,602,639 incorporated by reference, herein.

In operation, a standard frequency generator, well known to one skilled in the art, is connected to an electric and/or magnetic field transmitter, well known to one skilled in the art. For a complete discussion of designing magnetic and electric fields, see "Introduction to Electromagnetic Fields and Waves" by Erik V. Bohn, Addison-Wesley Publishing Co. (1968), incorporated by reference herein. The frequency generator controls and drives the electric and/or magnetic field transmitter which produces an electric and/or magnetic field. Opposing the electric and/or magnetic field transmitter in one embodiment, is an electric and/or magnetic field receiver. Between the electric and/or magnetic field transmitter and the electric and/or magnetic field receiver is a test zone defined by the transmitter's and receiver's location. The test zone is where the individual organism places a portion of himself or herself, such as a hand, so the hand is in the electric and/or magnetic field that exists between the electric and/or magnetic field transmitter and the electric and/or magnetic field receiver. The presence of the hand, or other portion, causes

the electric field and/or magnetic field to extend through the hand and the energy of the electric and/or magnetic field is affected in a unique way corresponding to the individual organism.

The electric and/or magnetic field receiver receives the  
5 electric and/or magnetic field. The detector produces a signal corresponding to the electric field and/or magnetic field received by the receiver and provides the signal to the microprocessor. The microprocessor has stored in its memory 113 a known electric and/or magnetic field signal for the individual organism. The  
10 microprocessor calls up the stored known signal and compares it to the signal provided to the microprocessor from the detector. If the known signal and the signal from the detector are substantially similar, then the individual organism is recognized.

The detector can measure phase, amplitude, frequency,  
15 waveform, etc., of the electric and/or magnetic field which extends through the test zone and the portion of the individual organism in the test zone. Either an electric field by itself, or a magnetic field by itself or a combination of both can be present for the test zone. If frequency is used for recognition, then preferably  
20 the frequency is DC to 500,000 Hertz. If current is used for recognition, then preferably the current is 1 microAmp to 4 mAmp. If potential energy is used for recognition, then the voltage is preferably 0.1 to 15 volts. If waveforms are used for recognition, then sine, ramped, square, or combinations thereof can be used.  
25 In regard to the use of an electric field for recognition,

preferably an electric field of 20 to 700V/m squared is used. In regard to the magnetic field for recognition, a magnetic field of between 100 mGauss to 10 Gauss is preferred.

Basically, the hand or other portion interrupts a steady  
5 electric and/or magnetic field, and the detector measures the amount of interruption. See, U.S. Patent Nos. 4,493,039; 4,263,551; 4,370,611; and 4,881,025, incorporated by reference herein. For an electric field, the measurements could be from the back of the hand straight through to the palmar surface, although  
10 it would depend on how the transmitter and receiver are positioned. If a sweeping motion of the hand is used through the test zone, straight through measurements would be obtained first for the thumb, and then for each of the fingers in sequence. This results in five sets of data. In regard to the magnetic field, placement  
15 of the hand in the test zone would interrupt the current induced in the secondary coil from the magnetic flux created by the primary coil, as shown in figure 14.

Preferably, the hand is used as an essential part of the current path. A current is induced by placement of the heel of the  
20 palm over a magnetic and/or electric field as shown in figures 15,16,17, and 18 in the embodiment of the apparatus 10, and the induced currents at the finger tips are detected, either with a magnetic and/or electric field sensor.

The present invention pertains to a method for recognition of an individual living organism's identity. The method comprises the steps of sensing electric and/or magnetic properties of the organism. Then there is the step of recognizing  
5 the organism from the properties.

The different embodiments described herein revolve about the fact that a subject organism by being somehow present in, or more specifically part of, a circuit that is either electrically based or magnetically based or a combination of both, interferes or  
10 affects the energy in that circuit in a unique way. By knowing how the subject individual interferes or affects the energy in the circuit a priori, and then testing again under essentially the same conditions how the subject individual interferes or affects the energy in the circuit, the test information can be compared to the  
15 previously identified information, and the identity of the subject individual can be either confirmed or rejected.

There are many ways this can be accomplished as described above. To summarize, these include but are not limited to the following. A touch technique which measures the electrical  
20 properties of the subject individual can be used. A touch technique which measures the magnetic properties of the subject organism can be used. A touchless technique which measures the electric and/or magnetic properties using steady electrical and/or magnetic field interruption can be used, as shown in figures 12,  
25 13, 14 and 21. A touchless technique which measures the

electric/magnetic properties using induced currents from an electric or magnetic field can be used, as shown in figures 15, 16, 17, 18, 20 and 22. A touchless technique which measures the electric/magnetic properties using steady electromagnetic field interruption can be used, as shown in figure 21. The touchless method which measures the electric/magnetic properties by reflection of an electromagnetic field can be used, as shown in figure 22, and where only one field is detected as shown in figure 23. A touchless technique which measures the electric/magnetic properties using induced current from an electromagnetic field can be used or an acoustic field as shown in figures 67-71. These are but some examples of how electrical or magnetic properties of an individual can be determined for recognition purposes.

The present invention pertains to an apparatus for recognition of an individual living organism's identity. The apparatus comprises a sensing mechanism having a contact area of less than 2.0 centimeters squared to identify an attribute of the organism. The sensing mechanism produces a signal corresponding to the attribute. The apparatus comprises a mechanism for recognizing the organism from the attribute. The sensing mechanism is in communication with the recognizing mechanism so the recognizing mechanism receives the signal from the sensing mechanism. Preferably, the recognizing mechanism is in contact with the sensing mechanism. The contact area of the sensing mechanism is preferably less than .2 centimeters thick. In the preferred embodiment, a single acoustic transducer having about a 1.5 cm<sup>2</sup>

surface area was used to detect a biometric recognition pattern. The acoustic transducer surface is less than 2 mm in thickness.

Figure 63 shows an actual size of a 1 cm diameter and 1.25 cm diameter thin electrode for sequential grasping between the thumb and fingers. Figure 64 shows a cross-sectional view of the electrode. Figure 65 shows a side view of the electrode. Figure 66 shows a flip-up sensor. This sensor can be only as thick as two pieces of metal foil and an insulator. It can be on a hinge so that it is flush with a surface until it is used. Then it is flipped up at right angles to the surface.

The present invention pertains to an apparatus for recognition of an individual living organism's identity. The apparatus comprises a sensing mechanism having a thickness of less than .2 centimeters to identify an attribute of the organism. The sensing mechanism produces a signal corresponding to the attribute. The apparatus comprises a mechanism for recognizing the organism from the attribute. The sensing mechanism is in communication with the recognizing mechanism so the recognizing mechanism receives the signal from the sensing mechanism.

The present invention pertains to an apparatus for recognition of an individual living organism's identity. The apparatus comprises a sensing mechanism for sensing an attribute of the organism. The sensing mechanism produces a signal corresponding to the attribute. The apparatus comprises a

mechanism for recognizing the organism from the attribute with an accuracy of greater than one in a billion.

In the preferred embodiment, 9 out of 10 imposters can be eliminated with a single frequency scan. There are significant  
5 electric/magnetic pattern differences at least every 50 Hertz. Scanning from 50 Hertz up to 500, 000 Hertz, yields 10, 000 significant patterns. If a different 9 out of 10 imposters are eliminated at every different frequency, then an accuracy is attained of 1 in 1 times 10 to the 10, 000 power of people. The  
10 entire world population is only 8 times 10 to the 9 power of people, rounding to 1 times 10 to the 10 power. Accordingly, an accuracy for 1,000 times the planet's population is attained. However, only a different 9 out of 10 imposters at 10 different frequencies are needed to be eliminated in order to be accurate for  
15 the entire world. The present invention is able to eliminate a different 9 out of 10 imposters for at least 25 different frequencies.

The present invention pertains to an apparatus for recognition of an individual living organism's identity. The  
20 apparatus comprises a sensing mechanism which is moldable into a shape having a non-flat surface. The sensing mechanism senses an attribute of the organism and produces a signal corresponding to the attribute. The apparatus comprises a mechanism for recognizing the organism from the attribute. The recognizing mechanism is in  
25 communication with the sensing mechanism. In the preferred

embodiment, the sensing mechanism can be concave, flat, convex, or a combination thereof, lending them to molding into numerous devices. The sensing mechanism simply needs to contact the skin of the subject individual. In a preferred embodiment, plastic  
5 piezoelectric material was used for the molded surface. Piezoelectric film sensors can be purchased from the AMP Piezo Film Sensor Unit in Valley Forge, Pa, incorporated by reference herein. Alternatively, see "Piezocomposite Transducers- A milestone in ultrasonic testing" by G. Splitt, incorporated by reference herein.  
10 In addition, rigid acoustic transducers can be curved concave, or curved convex, or beveled or faceted surfaces can also be used.

The present invention pertains to an apparatus for recognition of an individual living organism's identity. The apparatus comprises a sensing mechanism which is flexible. The  
15 sensing mechanism senses an attribute of the organism and produces a signal corresponding to the attribute. The apparatus comprises a mechanism for recognizing the organism from the attribute. The recognizing mechanism is in communication with the sensing mechanism. In a preferred embodiment, an acoustic biometric sensor  
20 made of plastic-type piezoelectric material, as identified above, can be used which results in a flexible sensing mechanism.

Preferably, the sensing mechanism is made of rubber, plastic, metal, mineral or ceramic or composites. Because an electrode need only to be able to contact the skin of the subject  
25 individual, the electrode surface can be flexible. By being able



to bend or compress, flexible electrodes can be built into a watch and its bands or jewelry or items of clothing, leather luggage or plastic credit cards without any affect on the functionality of the article being attached with the flexible electrode. For instance,  
5 there can be a plastic identity card with a name and picture, and a thumb electrode on one side and two or three finger electrodes on the other side. The card can be slid one quarter inch down into a reader and the electrodes grasped. The reader compares the pattern of the subject individual who is contacting the thumb electrode and  
10 two or three finger electrodes to the pattern stored on the card.

Referring to figures 24-33, there are shown the circuit diagrams regarding a preferred embodiment of the apparatus for recognition that can be connected to sensors or electrodes. Except as indicated, all decimal capacitance values are in  $\mu F$ , and all  
15 whole-number capacitances are in pF. All resistances are in ohms.

The system contains a waveform-generation stage, a waveform-detection stage, and associated digital logic. The system allows up to 8 connections to a person for measurement.

The frequency range of the waveform-generation stage is  
20 approximately 75 Hz to 1.2 MHZ. To generate this signal, a voltage-controlled oscillator (U13) is used. The voltage used to tune the oscillator is generated by U11, a 12-bit D/A converter. This converter conveniently uses a serial input, so only 3 wires are required from the microcontroller to set the voltage output

instead of the customary 12. The VCO tunes from approximately 300 kHz to 1.2 MHz, a coverage range of approximately 1 to 4. Output from the VCO is approximately a square wave.

The VCO is fed into a 12-bit ripple counter, U15, in order to make lower frequencies available. The ripple counter is wired to divide the VCO output frequency by powers of 4; e.g., the output frequency is divided by 1, 4, 16, 64, 256, 1024, or 4096. One of these outputs is selected by quad NAND gates U5 and U6. Each possible divisor is assigned to one input of its own NAND gate. The other input from each gate is set by the microcontroller to enable the correct divisor only. As the microcontroller has a limited number of pins, an 8-bit parallel output serial shift register, U14, is used to reduce the number of connections required from 7 to 2 by allowing the NAND gate mask to be transmitted serially from the microcontroller.

As the D/A and VCO sections may exhibit some frequency drift over time, one of the divider outputs is connected to one of the microcontroller I/O pins. This permits the microcontroller, which contains a time reference which is locked to a ceramic resonator, to determine the actual VCO frequency for calibration purposes. The accuracy of this determination is limited by the resonator's tolerance and is 1% or better.

The outputs of the NAND gates are shaped with RC filters to limit the spectrum of the output waveform to what is intended.

As square waves contain a very high-frequency component at the time of each state transition, the wave shapes are modified so that they are somewhat rounded. This ensures that the frequency being measured by the waveform-measurement stage is the frequency which  
5 was intended for measurement.

After the RC filters, the frequency-divided outputs are summed to a common point and passed through a capacitor to remove the DC bias. Note that only one output should be transmitted at a time (although it is possible to program the microprocessor to  
10 output multiple frequencies, this is not normal operation). The signal is fed, with the DC bias removed, to a CMOS analog multiplexer, U7, to distribute the signal to a point on the subject's hand; e.g., a finger or the wrist. The signal at this stage is approximately 1 volt peak to peak. U7, by the way, takes  
15 its address and enable inputs from another parallel output serial shift register, U9, for the same reasons that U14 is present elsewhere.

The waveform-measurement stage begins with a set of eight input amplifiers based on the LT1058 quad JFET input precision  
20 high-speed op-amp (U3, U4). Its pin-compatible with many other quad op-amps including the LM324. The LM324 cuts off around 20 kHz, and response past 1 MHz is needed. The voltage gain is set at 2:1 but can be adjusted by altering resistor values. The issue is ensuring that sensitivity is adequate without overloading the  
25 analog MUX inputs on U8. Remember that the full output of the

waveform-generation stage will be on one of the MUX pins, while the low level at another pin is being routed to the detector.

The CMOS analog multiplexer, U8, is used to route the signal from the appropriate hand connection (e.g., finger or wrist) to the detector. The address and enable inputs for this MUX also come from U9.

A half-wave diode detector is used to rectify the AF or RF signal and provide a DC level which is usable by the A/D converter. Because the diode has a forward voltage drop of around 0.3 V, a 0.3 V bias voltage is used to keep the diode at the threshold of conduction for small signal detection. The bias voltage is generated by reference to an identical diode.

The A/D converter, U10, is microprocessor compatible meaning that its outputs can be switched to high impedance. This permits the same connections to be used for other purposes. Of the eight output pins, seven are dedicated to the A/D converter, but one doubles as the data pin for the serial input chips, U9, U11, and U14. This works because the microcontroller lines are bidirectional, and the serial input chips are not clocked during A/D transfers to the microcontroller. To further complicate things, the ten A/D output bits are stuffed into eight wires, meaning two wires are used to read two bits each. This is accomplished by initiating two read cycles from the microcontroller.

The microcontroller, U16, is a BASIC Stamp II from Parallax, Inc. It has a built-in serial interface with a line receiver, "fakes" a line transmitter with a resistor (works for most computers, but some might have trouble as the logic levels aren't standard—see the documentation from Parallax), 16 I/O lines, 26 bytes RAM, 2048 bytes EEPROM, and a BASIC interpreter in ROM. The controller is very easy to use and programs in a BASIC dialect. It should be noted: pin 3 of U16 must be connected when programming the microcontroller, but must be disconnected immediately after programming and prior to use. This disconnection is shown on figure 33.

To read an impedance, the following steps must be performed by the microcontroller. This is generally in communication with a host computer such as a notebook computer running Windows 98 and appropriate software. The microcontroller software is already written, and serves to accept commands from the host computer and return readings as appropriate.

1. Set the D/A converter to output a voltage which causes the VCO to oscillate at the desired frequency. This is within a range of 300 kHz to 1.2 MHz. This step is performed by sending a 12-bit signal to the D/A converter via the 3-wire serial interface A0, A11, and A12.

2. The frequency output by the VCO should be measured by counting the pulses on the appropriate microcontroller pin (A13) over a fixed period of time. The D/A converter output can be adjusted as necessary to ensure that the correct frequency is produced.

(This step can be done either in real time, or more preferably as a pre-operation sequence to produce a frequency calibration curve. The unit will not drift appreciably during a usage session, but might over weeks or months. It also requires this frequency calibration prior to being placed in service. This step can be entirely user-transparent.)

3. The input and output MUX channels (fingers or wrist) must be selected. This is done by sending an 8-bit signal to U9 via the 2-wire serial interface A0 and A10.
4. The appropriate frequency divider output (1, 4, 16, 64, 256, 1024, or 4096) must be selected. This is done by sending an 8-bit signal (7 bits are used) to U14 via the 2-wire serial interface A0 and A14.

5. A brief settling time (10 ms is adequate) should occur to allow the capacitor in the signal detector to reach equilibrium with the new measured value.
6. The A/D converter is read. This is accomplished using A0 through A7 for data, A8 and A9 for control. The chip is actually read twice to obtain all ten bits of the result; refer to the manufacturer's documentation. Do not forget to set A0 as an input pin for this step; it is used at other times as an output pin for serial data.

The data read by the A/D converter will require numeric adjustment via some calibration curve to represent an actual impedance. This curve will be sensitive to frequency on account of the RC filters and frequency response of the input amplifiers, MUX, and signal detector circuit. A "calibration plug" with fixed impedances in place of a handpiece has been fabricated to allow the system to produce calibration curves for this purpose.

7. A15 is connected to a piezo buzzer to allow the microcontroller to make appropriate noises as desired by the programmer. Alternatively, A15 may be used to drive a small speaker through appropriate circuitry—the microcontroller can

generate as many as two audio frequencies at a time on this pin using pulse width modulation.

For a discussion regarding transducers and acoustics generally, see "Encyclopedia of Acoustics" by Malcolm J. Crocker,  
5 John W. Ley & Sons, Inc., incorporated by reference herein.

There are various embodiments for biometric units such as hand units 125 that are used for recognition purposes. These hand units can be used as a key to start or allow access to a computer, vehicle or other object. A signature signal is sent by wiring, or  
10 by transmission, to a computer. The computer processes the signal and either compares it to a known signature signal of the organism already stored in the computer's memory, or prepares it for further transmission to a remote location, or both. Alternatively, instead of simply allowing access or activating a computer once recognition  
15 is attained, a constant signal of the person holding or operating the hand unit, mouse or the keyboard can be sent from the computer through a modem either directly to a remote party or through the Internet to assure the party at the remote site that the person at the keyboard or mouse who is in communication with the remote  
20 party, is the desired person. In this latter scenario, the assurance is then maintained over time that the person who has the proper recognition to activate the computer does not then turn the control of the computer over to a third party who does not otherwise have access to the computer, and appropriate the computer  
25 for subsequent operations under the authorized persons name, such



as sending or obtaining information or purchasing goods or services from a remote location which requires the identity of the authorized person. The computer can also keep a log of who accessed a site and when.

5                Generally, six electrodes are used for hand units. All connections are made through the 9 pin connector that is standard on the back of a computer tower or desktop, although the 25 pin printer port can also be used. The pins used on the 9 pin connector are the same ones for each hand unit. The electrodes can  
10 be conductive metallic foil, plastic, or rubber. They can be flat (about 2 centimeters times 2 centimeters) or molded for finger tips (taking into account the large variations in size). For a simple hand unit that will be used for recognition, a flat reversible hand unit can be used for the right or left hand as shown in figures 34 and 35. Electrodes are placed in the following regions: 1) heel of the palm (a long electrode strip or a single small electrode movable on a spring); 2) thumb tip; 3) index finger tip; 4) middle finger tip; 5) ring finger tip; 6) little finger. The hand unit must be adaptable for large or small hands. It is made out of  
15 clear plexiglass for each surface. There is a hollowed out area for the heel of the palm to fit into, and also for the finger tips. The entire hand area could be hollowed out a little to produce more consistent hand placement. The hand piece is fabricated using brass inserts pressed through plastic sheets for the electrodes.  
20

In regard to a keyboard 126 as shown in figure 36, electrodes can be placed at the (t), (7), (9), (p) keys and a 4 centimeter strip can be placed on the left end of the space-bar and a palm strip on the lower frame of the keyboard. Conductive rubber  
5 keys for the keyboard, at least at these locations, would be preferred. This embodiment on a keyboard would be appropriate for activation as opposed to continuous indication of the presence of an authorized user, since the user would not be able to maintain contact with all the electrodes continuously. The wiring from the  
10 electrodes on the keyboard can run with the normal keyboard wiring to the computer, or to the 9-pin or 25-pin connections.

A mouse 128, as shown in figures 37 and 38 could also be prepared for recognition. Conductive foil strips or imbedded conductive polymers that attach flat to the surface of the mouse  
15 for the palm and each finger tip would allow easy grasping over time of the mouse. A variation of requiring the user to continually hold the mouse along the foil strips can be established, where a time period exists which requires the user to grip the mouse at least once during each time period so the  
20 computer is not shut off. The keyboard and mouse preferably use Compac aluminized tape with conductive adhesive for the electrodes. The wiring from the electrodes on the mouse can run with the normal keyboard wiring to the computer, or to the 9-pin or 25-pin connections.

A wrist band 129, as shown in figure 39, made of elastic material can be used to simulate a wrist watch. Electrodes can be conductive foil attached to the inside of the band. A transmitter of the wrist band can transmit the individual's signature obtained with the electrodes by the push of a transmission button or by periodic automatic transmission. The transmission of the signature will then be received by a device that will have or has access to the person's known signature, and recognition will then be confirmed or denied for whatever the application or purpose. For instance, the watch can be activated by proximity to a wall unit. The wall unit recognizes the watch and gives entry. For this, the wall unit would recognize the watch on the person. Basically, the whole transmission is proximity detected. The watch has a transmitter and receiver. The wall unit emits a radio signal which is received by the receiver of the watch, causing the watch to transmit the biometric signal. The wall unit receiver receives it and compares it with known authorized signatures. If a match occurs, the wall unit allows current to flow to a lock mechanism in the door, disengaging the door lock so the door can be opened. The wrist band could be used with a personal area network, see "Personal Area Networks: Near-Field Intrabody Communication" by T. G. Zimmerman, Systems Journal, Vol. 35, No. 314, 1996, MIT Media Lab, incorporated by reference herein.

In a preferred embodiment, and referring to figures 40-58, multidimensional matrices such as three and four dimensional matrices are formed for recognition purposes. Acoustic biometric

scans can produce three-dimensional patterns at one frequency, and four-dimensional patterns at multiple frequencies. The electric/magnetic techniques described herein produced two-dimensional scans at a single frequency and three-dimensional matrices when multiple frequencies are used in regard to a single segment of the subject organism. In the electric/magnetic techniques, if there are multiple sensors along the current path, such as shown in figures 40, 42 and 44 there would be for instance 8 different readings for the palm to thumb-tip current, at one frequency. That would produce a two-dimensional reading for the thumb and a three-dimensional plot for all five fingers. Extending this to multiple frequencies would yield a four-dimensional plot of the subject organism, as shown in figures 46 and 49. By varying the waveform and switching patterns, five and six-dimensional matrices as shown in figures 56-58 are attained.

Scans on the thumb of several people all at a single frequency resulted in unique signatures corresponding with the individuals which allowed for easy identification of the individuals. For a single frequency scan, in its simplest form, a two-dimensional plot was obtained, with amplitude on the Y axis, and time on the x axis as shown in figures 50 and 51. For a multiple frequency scan, a three-dimensional plot was obtained with frequency on the Z axis. The mode that was used to obtain the result was the "radar" type mode, with a single transducer working in what is known as the "pulse-echo mode". Preferably, only one

transducer was used and excellent results were achieved, although more than one transducer could have been used.

In the radar type mode, the acoustic energy was transmitted by the single transducer in contact with the skin of the subject organism. The acoustic energy was released essentially in a well defined short burst and as the energy passed through the subject organism, portions of it over time were reflected as the energy moved through the soft and hard tissue of the subject organism. The echo or reflection of the energy back to the transducer over time yielded the signature of the subject organism.

In its more complex and preferable form, three-dimensional scans were produced at a single frequency. One side of the thumb was scanned to the other, for a total of 25-35 scans per person. Each single scale was two-dimensional, and when combined in a group, with location plotted on the Z axis, yielded a three-dimensional ultrasonic topography of the thumb, as shown in figures 52 and 53. If the three-dimensional ultrasonic topography is extended to multiple frequencies, a four-dimensional plot results, with frequency on the W axis, as shown in figure 54. If waveform is varied, a five-dimensional plot results, as shown in figure 55.

In the preferred embodiment, medical frequencies in the low MHZ range (2.25 MHZ; 0. 7 to 1. 8 millimeters wavelength) were used and were able to detect all the detail necessary, and even

actually more than necessary, to obtain a unique signature. This is why a two-dimensional scan at a single frequency is able to be obtained.

It should be appreciated that although the detection of  
5 induced current can be used for biometric recognition, the  
detection of induced current can be used for other purposes such as  
for diagnostic purposes including bone. In a normal bone, an  
induced current will flow through the bone since the bone is a  
conductor, as is well known in the art. See, "Radiofrequency  
10 Radiation Dosimetry Handbook", Fourth Edition, October, 1986; USAF  
School of Aerospace Medicine, Aerospace Medical Division (AFSC),  
Brooks Air Force Base, TX 78235-5301, incorporated by reference  
herein. See figure 59. However, when the bone has a fracture or  
break in it, the current will be interrupted due to the break or  
15 fracture and will prevent the current from flowing or substantially  
reduce the current from flowing that would have otherwise flowed if  
the bone did not have a break or fracture. As shown in figure 61,  
an apparatus for inducing an electric current in the bone, as  
described above, can have a galvanometer which reads the current  
20 flow which is induced in the bone, or in the case of a fracture or  
break, the lack thereof. Figure 62 shows an apparatus to induce  
current in the bone with a galvanometer that shows expected and  
normal current flow through the bone.

The present invention pertains to an apparatus for  
25 identifying electric and/or magnetic properties of an individual

living organism. The apparatus comprises a sensing mechanism for sensing the electric or magnetic properties. The apparatus comprises a mechanism for forming matrices corresponding to the organism having at least four-dimensions.

5           The present invention pertains to an apparatus for diagnosing a bone. The apparatus comprises a mechanism for inducing a current in the bone. The apparatus comprises a mechanism for detecting a fracture or break in the bone.

10           The present invention pertains to a method for diagnosing a bone. The method comprises the steps of inducing a current in the bone. Then there is the step of detecting the induced current in the bone. Next there is the step of detecting a fracture or break in the bone.

15           The present invention pertains to a method for sensing an induced current in an individual living organism. The method comprises the steps of inducing current in the organism. Then there is the step of detecting the current induced in the organism. Preferably, the detecting mechanism detects a characteristic of the organism associated with the induced current.

20           The present invention pertains to an apparatus for sensing an induced current in an individual living organism. The apparatus comprises a mechanism for inducing current in the organism. The apparatus comprises a mechanism for detecting the

current induced in the organism. Preferably, the detecting mechanism detects a characteristic of the organism associated with the induced current.

5 The present invention pertains to an apparatus for sensing the electric and/or magnetic properties of an individual living organism. The apparatus comprises a mechanism for transmitting electric and/or magnetic energy into the organism. The apparatus comprises a mechanism for receiving the electric and/or magnetic energy after it has passed through the organism.

10 The present invention pertains to a method for using a computer. The method comprises the steps of sensing a non-visible attribute of an individual. Then there is the step of recognizing the individual. Next there is the step of accessing the computer by the individual.

15 The present invention pertains to a method for secure communication between an individual at a first location and a second location. The method comprises the steps of sensing a non-visible attribute of an individual. Then there is the step of recognizing the individual. Next there is the step of allowing the  
20 individual to communicate with the second location.

The present invention pertains to an apparatus for sensing the electric and/or magnetic properties of an individual living organism. The apparatus comprises a mechanism for



transmitting acoustic energy into the organism. The apparatus comprises a mechanism for receiving electric and/or magnetic energy generated in the organism due to the acoustic energy after it has interacted with the organism.

5           The present invention pertains to a method for sensing the electric and/or magnetic properties of an individual living organism. The method comprises the steps of transmitting acoustic energy into the organism. Then there is the step of receiving electric and/or magnetic energy generated in the organism due to  
10 the acoustic energy after it has interacted with the organism.

          Impedance and phase angle resonance frequencies can also be used for recognition. For instance, a person can grasp a transducer with the thumb and forefinger with the transducer providing a multifrequency scan point of the thumb and forefinger.  
15 Each organism for a given body segment has a unique impedance or phase angle resonance frequency that can be used to recognize the organism.

          Figure 67 shows the acoustic generation of direct current. An acoustic generating system provides energy to a  
20 piezoelectric material. The acoustic energy will travel through the body segments and a direct current will be generated. The direct current will be generated in the semi-conductor structures. Figure 68 shows the acoustic generation of alternating current and magnetic fields. An alternating current will be generated in the

semi-conductor structures whose natural oscillating frequency matches the acoustic frequency. This will in turn produce a magnetic field. Figure 69 shows the detection of direct current or alternating current induced by acoustic energy. The acoustic  
5 generating system is connected to the piezoelectric material which results in acoustic energy traveling through the body segments. In turn direct current results which is detected by electric field detectors such as capacitors. Figure 70 shows the detection of alternating current induced by acoustic energy. At a single  
10 frequency the locations are mapped out of the structures producing the alternating current, by detection with magnetic field detectors. Figure 71 shows an acoustic wave induced by electric and/or magnetic energy. The acoustic analysis system receives induced acoustic waves from an acoustic transducer which results  
15 from electric/magnetic energy interacting with the body segments that have arisen from an electric and/or magnetic transmitter.

Referring to figures 75, 76, 77, 78 and 79, the present invention pertains to an apparatus 199 for authenticating an individual. (The apparatus 199 for authenticating an individual  
20 can be the mechanism 135 for recognizing a biometric signature of the individual). The authenticating apparatus 199 comprises a contact card 170 having electrodes 150 which an individual touches to generate a biometric signature. The authenticating apparatus 199 comprises a reader 174 for the contact card 170 for reading the  
25 contact card 170 and recognizing the individual from the biometric signature.

Preferably, the contact card 170 provides a present biometric signature and the reader 174 causes the present biometric signature to be compared with a known biometric signature to recognize the individual. The card 170 preferably includes a first  
5 side 147 and a second side 148, and wherein the plurality of electrodes 150 includes a plurality of finger electrodes 151 disposed on the first side 147 which the individual touches with fingers, and a thumb electrode 153 disposed on the second side 148 which the individual touches with a thumb.

10 Preferably, the apparatus 199 includes a contact electrode 173 which contacts the reader 174, through which the present biometric signature is transferred to the reader 174 from the card 170. The reader 174 preferably includes a reader contact plate 183 that contacts the contact electrode 173 through which the  
15 present biometric signature transfers from the card 170 to the reader 174. Preferably, the reader 174 includes a groove 175 in which the card 170 is inserted for the contact electrode 173 to contact the contact plate 183. The contact plate 183 is disposed in the groove 175. The groove 175 preferably has an end 169 and  
20 wherein the reader 174 includes a stop 159 at the end 169 of the groove 175 to stop the card 170 so the contact electrode 173 and contact plate 183 align when the card 170 is inserted into the groove 175.

Preferably, the card 170 includes a card memory 172  
25 having the known biometric signature for providing the reader 174

the known biometric signature. The reader 174 preferably includes a memory reading mechanism 185 that reads the known biometric signature from the card memory 172. Preferably, the memory reading mechanism 185 is disposed in the groove 175, and the card memory 5 172 is disposed in the first or second sides of the card 170 so it can be read by the memory reading mechanism 185.

The reader 174 preferably includes a generator 177 which generates an electrical signal which is transferred to the contact plate 183, then to the contact electrode 173 and then to the finger 10 electrodes 151 and/or the thumb electrode 153 for generating the present biometric signal. The generator 177 is in connection with the contact plate 183.

Preferably, the authenticating mechanism 199 includes a mechanism 163 for comparing the known biometric signature with the 15 present biometric signature. The comparing mechanism 163 is preferably a computer 158. Preferably, the reader 174 includes a register 160 which stores the present biometric signature and the computer 158 is disposed in the reader 174 and connected to the register 160. The register 160 is connected to the contact plate 20 183.

Alternatively, the reader 174 includes a modem 197, which communicates with the computer 158, that is remote from the reader 174 and sends the present biometric signature to the computer 158. The modem 197 is in communication with the contact plate 183. If

desired, the computer 158 can be disposed in the reader 174 so the computer 158 causes the recognition to occur in the reader from the present biometric signature and the known biometric signature in the memory 172. The modem 197 is then used to communicate authentication.

Preferably, the card memory 172 is either a bar code 171, magnetic strip 179 as shown in figures 80 and 81, or both as shown in figures 86 and 87. It can also be a microchip memory 189, or a hologram or an optical memory, or any other memory mechanism convenient to dispose on a card. The memory reader mechanism 185 preferably includes either a bar code reader 179 as shown in figures 77 and 78, or a magnetic strip reader, or both as represented by the memory reader 185, as shown in figure 79. Alternatively, the memory reader mechanism is a hologram reader or microchip reader. The reader 174 can include a PIN entering mechanism 195 through which a PIN is entered into the reader 174. The reader 174 function depends on a predetermined PIN being entered into the reader 174.

Alternatively, the comparing mechanism 163 includes a microchip 189 disposed on the card 170 as shown in figures 75b, 79a, 79b, and 85. The microchip 189 is in connection with the card memory 172 and the contact electrode 173. The microchip 189 may control the generator 177 through the contact electrode 173 and contact plate 183. Alternatively, the authenticating mechanism 199 includes a microchip 189. Alternatively, the authenticating

mechanism 199 can include an antenna 187 and a microchip 189 for transmitting the present biometric signal to the reader 174 as shown in figures 78a, 88, 89 and 90.

In the operation of the invention, one general  
5 application of many possible applications for the biometric signature of an organism, is regarding authorization for an action. Once the organism, preferably a person, is recognized from the person's biometric signature, then an action, such as a lock opening or a purchase being charged, occurs. For example, the  
10 biometric signature of the person can be used in place of a credit card to charge a purchase.

In such an embodiment, any apparatus to obtain a biometric signature of a person can be used, but a sensor mechanism 123 that is preferably the hand unit 125 is used to obtain a  
15 biometric signature of a person as shown in figure 72. As described below, the person at a check station 149 simply places the person's hand on the hand unit 125 so the electrodes 150 contact the hand. The hand unit 125 obtains a biometric signature of the person and provides it to a signal processor 152 which  
20 converts the biometric signature from the hand unit 125 into a signal having a desired form, such as a digital signal, for transmission over a communication line 121. The signal processor 152 can be an analog to digital convertor. The signal processor provides the biometric signature of the person, now in digital  
25 form, to a transmitter/receiver 154 that is preferably adjacent to

and in contact with the signal processor 152. The transmitter/receiver 154 is preferably a modem. When the modem receives the digital signal of the biometric signature, the modem is activated and communicates over a communication line 121, such as a telephone line, to a reference station 156, similar to how credit cards are currently verified for transactions. The reference station 156 also has a transmitter/receiver 154, such as a modem, which receives the digital signal of the biometric signature and provides it to a computer 158. The computer 158 stores the digital signal of the biometric signature it has received in a register 160 and then searches a reference memory 162 which has previously been filled with known digital signals of authorized biometric signatures of authorized individuals.

The computer 158 searches the reference memory 162 for essentially the same digital signal of the biometric signature as was sent to it. When the computer 162 finds in the reference memory 162 the corresponding digital signal of the biometric signature which was transmitted to the computer 158, the computer 158 transmits back to the check station 149 a confirmation that the person providing the biometric signature is recognized and hence authorization or consent for whatever action is desired is granted. The response from the computer 158 can appear on a display 164, such as a monitor or a printer which prints out the response. If no corresponding biometric signature can be found in the reference memory 162, then the computer 158 transmits to the check station 149 that recognition is denied.

If the action is, for instance, to purchase an item, then when the digital signal of the biometric signature is sent to the computer 158, the total cost of the purchase can also be sent with the digital signal. When the computer 158 has found the  
5 corresponding digital signal of the biometric signature in the reference memory 162, the purchase price can be charged to a corresponding file 159 also maintained in the reference memory 162, see figure 72, with the person's biometric signature. This process is like the process using a credit card to charge a purchase except  
10 that there is no longer any need for the credit card to be carried. The person's inherent biometric signature replaces the need for a credit card.

Alternatively, when the confirmation is sent back to the check station 149 from the computer 158 for the person submitting  
15 the person's biometric signature, additional information, such as the person's name or birth date or Social Security number can also be sent back so a technician or employee operating the check station 149 can further confirm that the person using the hand unit 125 at the check station 149 is who the computer 158 says the  
20 person is. The information about the person can alternatively or in addition to the aforesaid information, be information about some specific aspect of the person. For instance, in a medical application, the medical history of the person can be provided including what prescriptions the person is using or what allergies  
25 the person suffers from. Alternatively, the information about the



person, such as their name, can be provided to the employee before obtaining the biometric signature.

More specifically, in regard to the card embodiment,

I. Contact Card - Contact cards must physically contact a card reader.

A card, may contain memory only, memory and sensors, and memory and/or sensors, and /or microprocessors. Memory mechanisms 172 include but are not limited to:

- A. Data storage
  - bar code
  - magnetic strip
  - embedded microchip (smart card)
  - hologram
  - electric ink
  - pin index system
  - optical memory

B. Sensor card systems

- 1. Memory sensor card - Card contains memory 172 and sensors (bar code, magnetic strip, microchip, etc.). The generator control is in the card reader. Biometric analysis can take place in the card reader, or remotely.

2. Microprocessor sensor card - The card contains a microprocessor as well as memory and sensors. The generator control and analysis can be in the card (microprocessor card), the card reader, or remotely performed.

3. Sensor card - The card contains sensor(s) only and simply replaces a hand unit.

#### Electric/Magnetic Characteristics

C. Example for Bar Code - The card 170 (Fig. 75 (front) and 76 (back)) bears a bar code 171, which contains information on the impedance pattern. The card 170 also has electrodes 150 (preferably gold plated) for the thumb and three fingers, connected to a contact electrode 173 (also preferably gold plated). In one embodiment, the card user grasps the card 170 on the finger electrodes 151 and thumb electrode 153, and swipes the card 170 through the reader (Figs. 77 and 78), which obtains the known impedance pattern from the bar code 171. At the end of the groove 175, the user then rests the card 170 in the reader 174 for a few seconds. During those seconds, the reader 174 generates an electrical signal which is sent through the contact electrode 173 to the finger electrodes 151 and/or thumb electrode 153. The reader 174 reads the impedance pattern generated from the finger electrodes 151 and/or thumb electrode 153, again via the contact electrode 173. The reader 174 compares the present impedance pattern with the pattern obtained from the bar code 171 on the card

170 (Fig. 79). If the present and known biometric impedance patterns are sufficiently similar, the user is approved. The card 170 can be of a type which stores pre-paid credit and does not require connection by modem to another computer.

5           It can work like current credit or debit cards that also require processing by modem, as shown in figure 79. In such an embodiment, a card 170 is used to obtain a biometric signature of a person. As described above, the user grasps the card 170 so the electrodes 150 contact the fingers and thumb. First, the user  
10 swipes the card 170 through the groove 175 in the reader 174. The memory reading mechanism 185 in the reader 174 reads the information stored in memory on the card and provides it to a register 160, in a computer 158 in the reader 174. The user then rests the card 170 in the card reader 174, so that the contact  
15 plate 173 on the card 170 is in contact with the contact plate 183 in the reader 174. The reader obtains a biometric signature of the person and provides it to a computer 158. The computer 158 compares the biometric signature it has received with the biometric signature in the register 160. If the two signatures are  
20 sufficiently similar, the computer 158 transmits to the display 164 a confirmation that the person providing the biometric signature is recognized and hence authorization or consent for whatever action is desired is granted. If the biometric signatures are not sufficiently similar, then the computer 158 transmits to the  
25 display 164 that recognition is denied.

In another embodiment, instead of containing the actual electric/magnetic pattern, the bar code 171 contains a numerical index, number, pattern, or cypher based on the electric/magnetic pattern. When the electric/magnetic pattern is generated, the  
5 reader converts it through a predetermined algorithm into the numerical index, number, pattern, or cypher. The two indices, etc. are then compared, rather than the actual electric/magnetic patterns.

In another embodiment, the actual electric/magnetic  
10 pattern or index can be processed only if a unique user PIN number is provided.

In another embodiment, the unique user PIN number is used mathematically in the predetermined algorithm to determine the numerical index, number, pattern, or cypher.

15 In another embodiment, the card's memory contains information on the user name and account number only. Obtaining the known impedance pattern and performing the comparison must be done by modem with a remote computer shown in figure 22. In this instance, the reader 174 simply generates the current biometric  
20 pattern and transmits the resulting electrical measurements to the remote computer.

D. Acoustic Characteristic Example - The acoustic smart cards 170 (Fig. 74a, 75a (front) and 76b (back)) has a microchip

189, which contains information on the acoustic pattern. The cards 170 also has a transducer connected to the microchip 189. In one embodiment, the card user grasps the card 175 on the transducer, and swipes the cards 170 through the reader (Figure 74a), which  
5 obtains the known acoustic pattern from the microchip 189 via the contact electrode 173 (an acoustic biometric system with an acoustic card is shown in figure 77a). At the end of the groove 175, the user then rests the card 170 in the reader 174 for a few seconds. During those seconds, the reader 174 generates an  
10 electrical signal from the generator 177 which is sent through the contact electrode 173 to the transducer. The reader 174 reads the acoustic pattern generated from the transducer, again via the contact electrode 173. The reader 174 compares the present acoustic pattern with the pattern obtained from the microchip  
15 memory 189 on the cards 170. If the present and known biometric acoustic patterns are sufficiently similar, the user is approved. The cards 170 can be of a type which stores pre-paid credit and does not require connection by modem to another computer.

A contactless smart cards 170 can be used through antenna  
20 187a, 187b and transceivers which communicate, as shown in figure 78a. All of the various embodiments for electric/magnetic cards can be used with acoustic cards or any other type of sensor card.

E. Magnetic Strip - The card 170 (Figs. 80 and 81) bears a magnetic strip 129, which contains information on the  
25 biometric pattern. The card 170 is swiped through a magnetic

reader, rather than a bar code reader as above. Otherwise, use of the card is virtually identical to the bar code card. The electrical contact electrode must be placed at sufficient distance from the magnetic strip to prevent disruption of the magnetic  
5 strip.

F. Memory Microchip (Smart) Card 170 - The card (Figs. 82 and 83) is embedded with a small (preferably gold plate) contact electrode 173. When the card 170 is inserted into a smart card reader (no swiping is necessary, rather simple insertion is  
10 sufficient). The contact electrode 173 contacts the contact plate 183. In one embodiment, the generator control is in the card reader. The contact electrode 173 transfers information to the reader as described above (Fig. 84). Current generation through the contact electrode to the sensor(s) takes place, with subsequent  
15 reading and analysis of the biometric pattern, as described above.

G. ID card - The card bears a memory with information on the biometric signature of the user whose name appears on the front of the card. The card interacts with a sensor/memory reader, and the present biometric signature is obtained, as above. The card  
20 authenticates the identity of the user for completion of an action. This is essentially the same schematic as in Figure 79.

H. Microprocessor (Smart) Card - In this embodiment, the smart card 170 does not have to transfer information to the reader on the known biometric pattern or index. Instead, it may transfer

directions to the reader on scanning parameters (Fig. 79). The reader is simply the sensor energy generator and reader, but control of the scanning parameters rests with the smart card. The reader 174 generates the biometric scans in the generator 177, and  
5 relays the information on the scans to the microprocessor 138 on the smart card. The smart card then compares the pattern or index relayed by the reader with the pattern or index in its embedded memory 172. If there is sufficient agreement between the present pattern and the pattern in memory, the card signals to the reader  
10 that the user is authorized, and the reader signals approval to the user. The microprocessor may function as a simple memory chip, or may assume one or more functions of the reader, computer, register, generator and/or display.

In one embodiment, the scanning parameter directions  
15 contained in the smart card are fixed. In another embodiment, the scanning parameter directions in the smart card can be changed by the user, by insertion of the card into a scanning setter maintained by the user or a commercial enterprise. The user could:  
1) program specific frequencies and scanning patterns; 2) choose  
20 from one of several scanning programs, the details of which are not known to the user (i.e. the user would choose one scanning program from programs 1 through 100); 3) the user could program the smart card to randomly change its scanning pattern after every use.

In another embodiment, the sensor generator scanning  
25 control rests within the microprocessor on the smart card. The

reader serves merely as an energy source and possibly a display mechanism for authorization.

I. Hybrid Card - The hybrid card 170 (Figs. 86 and 87) contains more than one memory system, such as a bar code, magnetic  
5 strip, and microchip, all on the same card. It functions as described above, such as either a simple memory card, or as a combined memory/microprocessor card, or as a sensor/memory card.

In another embodiment of the hybrid card 170, the card is very similar to current credit cards and contains a signature line  
10 and the familiar magnetic strip. It also contains sensors such as a transducer or electrodes for the fingers and thumb, and a contact plate. The user can use it like a regular credit card at those locations that do not have sensor (acoustic or electric/magnetic) readers. At those locations that do have sensor (acoustic or  
15 electric/magnetic) readers, the rendering of a written signature is unnecessary.

## II. Contactless Cards

These cards look just like plastic credit cards, however, there is an embedded microchip 189 and an antenna 187, that allow  
20 the card 170 to communicate with an antenna/coupler unit without actual physical contact with a reader (figures 88, 89 and 90). The contactless biometric sensor card works much the same way as the contact card. The primary difference is in the coupling between



the reader and the card. With the contact card, a contact plate on the card comes in contact with a contact plate on the reader. There is a direct electrical connection which allows reading of the biometric pattern.

5           In the contactless card 170, its antenna 187 communicates with and obtains power from the antenna in the coupler unit. The EM field generated by the antenna in the coupler unit produces induced current in the card microchip and sensor system. These induced currents measure the biometric pattern and the microchip  
10 communicates the readings via the antennae 187 to the coupler/reader 174. This is a wireless system. The system in the card is called a tag (an electronic device that can communicate with a reader by means of a radio frequency signal.) Figures 88 and 89 show what a contactless electric/magnetic sensor card would  
15 look like. Figure 90 shows schematics for a contactless system.

For more information about "smart cards" generally, see [www.gemplus.com](http://www.gemplus.com); IBM smartcard solutions by IBM; Javacard solutions by Javasoftware, Inc.; a subsidiary of Sun Microsystems; Zone Development, Inc. of San Diego, Ca.; Environics Communications,  
20 Inc. at [www.environics.net](http://www.environics.net) about the smart card forum; Smart Card International, Inc. of Daytona Beach, FL; all of which are incorporated by reference herein.

The embodiments described above for sensor cards can be used with other sensor devices such as watch bands, gloves, glasses and other portable or detachable sensor mechanisms.

5 The present invention pertains to an apparatus for authorizing an action. The apparatus comprises a mechanism for recognizing a biometric signature of an individual. The apparatus comprises a mechanism for allowing the action.

10 The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of the individual. Then there is the step of allowing the action to occur. Preferably, after the allowing step there is the step of performing the action.

The action can include, but is not limited to:

I. Financial Transactions

- 15 Banking and payment  
Gaming  
Utilities and metering  
Mass transit and toll  
Payphones  
20 Healthcare and social services  
Wireless communications  
Pay TV  
Education  
Travel  
25 Information technology  
Access control systems; or

II. Information technology

Loyalty and retail systems  
Government ID  
Identification  
Time card systems  
Healthcare and social services  
Financial transactions  
Access control systems; or

III. Access control systems

Locks  
Vehicles  
Remote controllers  
Closed environments  
Security  
Healthcare and social services  
Information technology  
Financial Transactions  
Communications

IV. Electronic tagging

House arrest  
Locator

Biometric authentication can be done in two modes -  
identification or verification. Examples of methods and systems  
using each mode are discussed in the examples below. It should be  
understood that authentication for a particular purpose can  
sometimes be achieved using either mode. For instance, access to  
an account at an ATM can be obtained in identification mode by the  
bank's computer searching for a match to the customer's present  
biometric pattern. In verification mode, the customer types in  
their name, and the bank's computer compares the customer's  
present biometric pattern with only one biometric pattern - the

customer's known pattern on file - rather than searching the entire database.

The authentication determination can be made using a variety of sensor 333 housing arrangements, including but not limited to: 1. Sensor(s) 333 and reader 174 housed in the same unit, as shown in figure 94; 2. Sensor(s) 333 and reader 174 housed separately, as shown in figure 95, and communicating directly through mechanisms including but not limited to contact electrode 183, wire, fiberoptic cable, modem 197, and such; and 3. Sensor(s) 333 and reader 174 housed separately, and communicating wirelessly through mechanisms including but not limited to infrared (IR), radio waves, microwaves, sound waves, contactless, and such. Examples of each sensor 333 housing arrangement are discussed below. It should be understood that authentication for the same purpose can be achieved using different types of sensor 333 housing arrangements. For example, access to an account at an ATM to withdraw money can be authenticated by a device built into the ATM, housing both reader 174 and sensor(s) 333. The customer could insert a separate sensor 333 bank card into the ATM, which communicates with the ATM reader 174 through a contact electrode. Alternatively, the sensor 333 bank card could be a contactless smart card which communicates with the ATM reader 174 wirelessly, via a radio frequency transmission.

The authentication determination can be made by a variety of reader 174 housing arrangements, including but not limited to:

1. reader 174 and determining mechanism 293 housed in the same unit, as shown in figure 96; 2. reader 174 and determining mechanism 293 housed separately, as shown in figure 97, and communicating directly through means such as wires, fiberoptic, cables, modems 197, and such; 3. reader 174 and determining mechanism 293 housed separately, and communicating wirelessly through means such as infrared (IR), radio waves, microwaves, and such. Examples of each reader 174 housing arrangement are discussed below. It should be understood that authentication for the same purpose can be achieved using different types of reader 174 housing arrangements. For example, access to an account at an ATM to withdraw money can be authenticated by a reader 174 and determining mechanism 293 which are both housed in the ATM. A reader 174 in the ATM could communicate by modem 197, with the bank's separately located central computer 158. The reader 174 in the ATM could communicate by microwave transmission with the bank's computer 158.

Biometric memory storage devices for known biometric patterns can be housed in a wide variety of ways. These can be grouped in four categories: 1. Memory 162 housed with sensor 333 device, as shown in figure 98; 2. Memory 162 housed with reader 174, as shown in figure 99; 3. Memory 162 housed with determining mechanism 293, as shown in figure 100; 4. Memory housed separately, as shown in figure 101. Each general category is discussed in more detail in the examples below. It should be understood that biometric authentication for the same purpose can be accomplished

using memory storage devices in more than one memory housing category. For instance, access to an account to withdraw money could be authorized by inserting into an ATM reader 174, a simple plastic card with biometric sensor(s) 333, and magnetic strip  
5 memory, containing the account number and known biometric pattern. Secondly, the ATM reader 174 could house a memory storage device for all biometric patterns of authorized account users, and make the determination. Thirdly, the ATM reader 174 could send the present pattern to the bank's central computer 158, which stores  
10 the known biometric pattern and makes the comparison. Finally, the reader 174 could send the present pattern to the bank's central computer 158, which in turn communicates with a separate known biometric pattern memory storage device. There can be a sensor 333, reader 174 and determining mechanism 293 in the same housing,  
15 as shown in figure 102, a sensor 333, reader 174 and memory in the same housing, as shown in figure 103, a reader 174, determining mechanism 293 and memory in the same housing, as shown in figure 104, a sensor 333, reader 174, determining mechanism 293, and memory in the same housing, as shown in figure 105, or a sensor  
20 333, determining mechanism 293, and memory in the same housing, as shown in figure 106.

Biometric authentication can be powered using a wide variety of power systems. These can be grouped in 3 categories: 1. Electrical power from the national power grid, such as from an  
25 outlet; 2. Electrical power from batteries (including rechargeable batteries); and 3. Electrical power converted from mechanical

energy. Each general category is discussed in more detail in the examples below. It should be understood that biometric authentication devices can be powered by more than one type of power system. For instance, access to an account to withdraw  
5 money could be authorized by an ATM reader 174 powered by direct electrical supply from the utility company power grid. The ATM reader 174 could also be powered by batteries inside the ATM. Lastly, the reader 174 could be powered by electricity generated mechanically by turning a handle.

10 Biometric identification or verification can be performed using a wide variety of sensor 333 installation arrangements. These arrangements can be grouped in four general categories: 1. Stationary merchant devices; 2. Portable merchant devices; 3. Stationary customer devices; and 4. Portable customer devices.  
15 Each general category is discussed in more detail in the examples below. It should be understood that biometric identification or verification for the same purpose can be accomplished using sensor 333 installation arrangements in more than one category. For instance, access to an account to withdraw money could be  
20 authorized by biometric sensors 333 built into an ATM machine. The sensors 333 could be in a portable reader 174 carried by a personal banker who makes house calls. The sensors 333 could be in a reader 174 built into the account holder's computer 158. Finally, the sensors 333 could be in a bank card the account holder carries  
25 around.

The sensors 333 can perform biometric identification or verification using a wide variety of energy fields. These fields can be grouped in four general categories: 1. Acoustic; 2. Electric; 3. Magnetic; and 4. Electromagnetic. Each general  
5 category is discussed in more detail in the examples below. It should be understood that biometric identification or verification of the same biophysical pattern can be accomplished using fields in more than one category. For instance, withdrawal of money from an account could be authorized by determining the biometric impedance  
10 pattern of the account holders' hand using acoustic fields. Likewise, this could be done using electric fields, magnetic fields, or electromagnetic fields.

The sensors 333 can obtain biometric information in two different user modes: touch and touchless. Each user mode is  
15 discussed in more detail in the examples below. It should be understood that biometric identification or verification of the same biophysical trait can sometimes be accomplished using either user mode. For instance, withdrawal of money from an account could be authorized by determining the biometric impedance pattern of the  
20 account holders' hand using touch electrodes. Likewise, this could be done using a touchless electric field hand sweep device.

Biometric identification or verification can be performed using sensors 333 with a wide variety of unique characteristics. These characteristics can be grouped in six general categories: 1.  
25 Size; 2. Thickness; 3. Accuracy; 4. Moldability; 5. Flexibility;



and 6. Matrices with four or more dimensions. Each general category is discussed in more detail in the examples below. It should be understood that biometric identification or verification of the same biophysical pattern can be accomplished unique characteristics in more than one category. For instance, a multi-frequency reader 174 for plastic cards using thin metal foil electrodes that are 2 mm in diameter, is unique for accuracy, matrices, flexibility, thickness, and size. It should also be understood that biometric authentication can be accomplished by different sensor 333 devices that use the same unique characteristic. For example, access to a bank account at an ATM to withdraw money can be achieved with a flexible smart card fitted with biometric electrodes. Money can also be withdrawn using a biometric wristwatch, the flexible band of which is fitted with biometric electrodes.

Biometric identification or verification can be performed using sensors 333 housed in a manner to be either operational or non-operational. An example of an operational sensor 333 is an acoustic transducer on the thumb flap of a door handle. When the user proceeds with the customary operation of the door, i.e. depressing the thumb flap to open the door, the biometric system is activated and the biometric boneprint pattern read and verified, and the door opened. An example of a non-operational sensor 333 would be a hand piece placed on the wall next to the door. The user first places their hand on the hand piece sensor 333 for authentication, and then moves their hand to the door to open it.

Biometric identification or verification can be used to authorize a wide variety of actions. These actions can be grouped in four general categories: 1. Financial transactions; 2. Information technology; 3. Access control systems; and 4. Electronic tagging. Each general category is discussed in more detail in the examples below. It should be understood that authorization for a particular action can involve more than one category. For instance, access to an account at an ATM to withdraw money is a financial transaction. It also involves information technology and access control because the account information is stored in an information storage device with controlled access.

Authorization of an action is achieved by an action mechanism 335, in communication with the determining mechanism 293. The action mechanism 335 can be: 1. housed with the determining mechanism 293, as shown in figure 107; or 2. housed separately from the determining mechanism 293, as shown in figure 108. Each action mechanism 335 housing category is discussed in more detail in the examples below. It should be understood that the same types of biometric authentication devices can be housed differently in regards to the action mechanism 335. For instance, authorization to open a door could be achieved by handle electrodes, reader 174, memory 162, determining mechanism 293, and action mechanism 335 (door unlock) in the door handle/lock mechanism. Similarly, the electrodes, reader 174, memory 162, and determining mechanism 293 could be installed in a hand unit on the wall next to the door, in communication with the action mechanism 335 (door unlock) in the

door handle/lock mechanism. Thus, one or more mechanisms making up a biometric authentication device or method- the sensors 333, reader 174, memory 162, determining mechanism 293, or action mechanism 335- can be integral within the same housing or device.

## 5 EXAMPLES

### I. Financial Transactions

A. Banking and payment - ATM's, drive through tellers, and indoor tellers can be equipped with hand units with six round electrodes, 1 mm thick and 2 mm in diameter. Biometric  
10 authorization could be required for a bank customer to deposit, withdraw, or transfer funds from a checking, savings, money market, CD, credit card, debit card, stored value card, or other type of account. The customer places their hand on the hand unit electrodes, which reads the biometric pattern. The present pattern  
15 data is communicated to the ATM or teller computer 158, as shown in figures 109, 100, 112, 113, or by modem 197 or wireless means to another bank computer 158, for comparison with the known biometric pattern on file, as shown in figure 111. This can be done in either identify or verify mode. Matching of the biometric pattern  
20 authorizes the customer to proceed with the banking action.

Bank cards 170 with sensors 333 can be used in place of hand units. For instance, the biometric pattern might be the acoustic pattern from the bone at the end of the thumb, as shown in figure 114. Piezoelectric plastic, 1.5 cm<sup>2</sup> in area, functions as a

transducer and is molded into the flexible card. The banking customer places the card into a contact reader 174, with their thumb touching the transducer. The reader 174 obtains the known biometric pattern from the card memory 172 (verify mode) and  
5 compares it to the present biometric pattern. The card is credit card sized and can be carried by the customer.

An Ohio customer wishes to bank in the Virgin Islands. He establishes a checking account with a Virgin Islands bank, which requires biometric authorization. The bank customer connects via  
10 direct computer 158 connection with the Virgin Islands bank computer 158 and sends his present biometric pattern, via touch electrodes molded onto his computer 158 keyboard keys 126, to the bank computer 158, as shown in figure 115. The keyboard electrode reader 174 uses 12 different AC frequencies providing accuracy of  
15 one in ten billion. The bank computer 158 compares the customer's known biometric pattern 162 with the present pattern (verify) to authorize the customer to make electronic payments from his checking account. Alternatively, the customer simply sends his present biometric pattern to the bank computer 158, and it searches  
20 its database for a match, to allow him access to his checking account (identify mode).

A person wishes to obtain cash from a credit union kiosk, as shown in figure 116. The kiosk is equipped with a number pad and a touchless biometric sensor 333. The sensor 333 is C-shaped,  
25 with an electric field between the C arms. The person inputs their

birthday on the keypad, allowing the reader 174 memory to restrict its identify search to only patterns with that birthday. The person next sweeps their right hand between the sensor 333 arms. The interruption to the electric field caused by their hand passing  
5 through the field produces a present biometric pattern which is matched to the known pattern 162 on file in the kiosk. Upon matching present and known biometric patterns, the person is given access to their accounts. In an alternate preferred embodiment, the apparatus includes a first account and a second account, and  
10 the action is a financial transaction between the first account and the second account and the allowing mechanism includes a mechanism for allowing the financial transaction. Preferably, the allowing mechanism allows the transfer of equities between the first account and the second account. Alternately, the allowing mechanism  
15 preferably allows a transfer of money between the first account and the second account. The transfer of equities or the transfer of money, in and of itself, is well known in the art, except that the biometric signature with the recognizing mechanism 135 is used to control whether the transfer can occur or not.

20 Referring to figure 72, the present invention pertains to a method for conducting a financial transaction. The method comprises the steps of identifying a financial transaction having a purchase price which a purchaser desires to execute. Then there is the step of recognizing a biometric signature of the purchaser.  
25 Next there is the step of charging an account of the purchaser with the purchase price.

Preferably, the financial transaction is a purchase. The recognizing step preferably includes the steps of obtaining a present biometric signature from the purchaser; and comparing a known biometric signature of the purchaser with the present  
5 biometric signature.

Preferably, the charging step includes the step of locating the account of the purchaser from the purchaser's present biometric signature. The charging step preferably includes the step of sending the biometric signature from a check station 149 to  
10 a reference station 156 via telecommunications lines 121.

Preferably, the sending step includes the step of sending the biometric signature and the purchase price over the telecommunications lines 121 and finding the account of the purchaser at the reference station 156. The obtaining of a  
15 biometric signature step preferably includes the step of placing a hand of the purchaser in communication with a hand unit 125 at the check station 149 which obtains the biometric signature of the person.

20 Referring to figures 91 and 72, the present invention pertains to an apparatus 133 for charging a purchase. The apparatus 133 comprises a mechanism 135 for recognizing a biometric signature of a purchaser. The apparatus 133 comprises a mechanism 137 for charging an account of the purchaser with the

purchase price. The charging mechanism 137 is connected to the recognizing mechanism 135.

Preferably, the recognizing mechanism 135 includes a mechanism 139 for obtaining a present biometric signature from a purchaser, and a mechanism 163 for comparing a known biometric signature of the purchaser with the present biometric signature of the purchaser. The comparing mechanism 163 is in communication with the obtaining mechanism 139. The obtaining mechanism 139 preferably includes a hand unit 125 which is adapted to receive the hand of the purchaser to obtain the biometric signature of the purchaser. The hand unit 125 is in communication with the comparing mechanism 163. Preferably, the comparing mechanism 163 includes a memory in which the known biometric signature of the purchaser is stored.

The account of the purchaser can be a bank account. The apparatus 133 for charging a purchase can include a control unit 166 in communication with the comparing mechanism 163 in which the purchaser identifies an amount of cash to be distributed to the purchaser, and a mechanism 141 for distributing cash disposed adjacent with the obtaining mechanism 139 and in communication with the comparing mechanism 163. The account is not limited to a bank account, but can be a brokerage account or any other account involving finances. The application described herein can be used for credit cards, debit cards, ATMs, checks, or any system in which

a financial transaction and the recognition of an individual in some way are desirable.

In another alternative embodiment, when the person places his or her hand on the hand unit 125, the person can also tell the employee operating the check station 149 the person's name. When the biometric signature as a digital signal is sent to the computer 158, the employee can also send the person's name by entering it through a control unit 166 connected to the modem at the check station 149. When the computer 158 receives the name, instead of searching all the digital signals of biometric signatures in the reference memory 162, the computer 158 can search by name the reference memory 162, and when the name is located, the biometric signature that was sent with the name can be compared to the stored known biometric signature with the name in the reference memory 162 to verify the identity of the person submitting the biometric signature.

In yet another alternative embodiment and referring to figure 73, instead of the person placing the person's hand on the hand unit 125, an employee at the check station 149 can provide a small sensor unit 170 to a person wishing to receive authorization. The sensor unit 170 has biometric sensors such as at least two preferably several electrodes 150 on it or a transducer, and a sensor unit memory 172. When the person holds the sensor unit 170 and places the person's fingers on the electrodes 150 or transducer, a signal is stored in the sensor unit memory 172. The



employee then takes the card 170 back and inserts it into a reader 174 which downloads the biometric signature stored in the sensor unit memory 172. The process regarding confirmation of the biometric signature then proceeds as described above. In the  
5 alternative, a portable sensor memory unit can use a touchless sensor system.

Instead of using a communication line 121 to contact a computer 158 at a reference station, there can be a computer 158 at the check station 149 and a reference memory 162 in contact with  
10 the computer 158 at the check station 149, as shown in figure 74. In this way the need for a communication line 121 is eliminated. The procedure is similar to that described above except that no transmission or reception between remote locations is necessary. The computer 158 will simply search the reference memory 162 at the  
15 check station 149 for the biometric signature of the person requesting authorization and either upon finding the biometric signature in the reference memory 162, provide authorization to the person, or upon not finding the biometric signature in the reference memory 162, deny authorization to the person. At  
20 predetermined times, for instance once a day or once a week, the reference memory 162 at the check station 149 can be updated by a CD or DVD or by a communication line downloading the latest list of authorized biometric signatures into the reference memory 162, as is well known to one skilled in the art.

B. Gaming - An Ohio gambler wishes to bet in Las Vegas. He establishes an internet account with a Las Vegas casino which requires biometric authorization to place a bet, as shown in figure 121. The gambler connects over the internet with the casino  
5 computer 158 and sends his biometric pattern, via his computer 158 mouse with molded, 1 mm thick, touch acoustic index finger transducer, to the casino computer 158. The casino computer 158 compares the gambler's present biometric pattern with the known pattern 162 (in either identify or verify mode) to authorize the  
10 placing of the bet.

A casino/hotel flexible card molded with four touch electrodes (2 mm diameter and 0.5 mm thick) can be issued to customers, as shown in figure 118. The card also functions as a room key. The casino/hotel card readers 174 use 5 frequencies,  
15 with sine and ramped waveforms at each frequency, producing a 4 dimensional biometric matrix. Anywhere the customer goes in the casino/hotel complex, the card can be used to pay for items and bill them to his room account. A line of credit with a dollar limit is also stored in the card for gambling purposes. The  
20 gambler wishes to obtain \$1,000 of chips to gamble. He places his electrode card, as shown in figures 117 and 118 in an automatic chip dispenser, grasping the electrodes. The reader 174 in the chip dispenser obtains his present biometric pattern and compares it to his known pattern (which is stored either in the casino  
25 computer 158, the reader 174, or the card), as shown in figure 117, figure 119 and figure 118, respectively. If the patterns match he

is authorized to receive the \$1,000 of chips. When the gambler returns to his room, he grasps the electrodes on the card and places the card in a groove on the lock mechanism. The lock mechanism compares his present and known biometric patterns, and  
5 upon finding a match, unlocks his door, as shown in figures 117, 118 and 119.

The gambler eats in the casino restaurant, but has forgotten his electrode card in his other suit. The waiter has a portable touch electrode card with embedded battery and  
10 microprocessor, and with electrodes 2 mm in diameter and 0.5 mm thick), as shown in figure 120. He brings the portable electrode card to the gambler's table. The gambler grasps the electrodes. The card stores his present biometric pattern. The waiter takes the card back to a determining mechanism 293, which compares (in  
15 either identify or verify mode), the gambler's present biometric pattern with his known pattern. The patterns match and the meal is billed to the gambler's account. When he returns to his room, he grasps the door handle (which is also fitted with electrodes) and upon matching biometric patterns enters his room, as shown in  
20 figure 122.

A video arcade issues biometric touch electrode wristbands (with enclosed microprocessor) to all customers entering the arcade, as shown in figure 123. Their biometric wristband pattern is stored in the arcade cash register computer 158, which  
25 is in communication with all the video games. When a customer

wishes to play a game, they hold their wristband near a small RF transmitter/receiver on the front of the game and press a button. The RF transmitter/receiver sends energy to the wristband microprocessor, creating induced current flow, which in turn causes  
5 the wristband to obtain the biometric wrist pattern and relay the pattern to the transmitter/receiver. This mode is similar to the contactless smart cards. The pattern is communicated to the cash register computer 158, which identifies the customer, and bills the game to the customer's account. This way no tokens or coins are  
10 needed to play the games. When the customer leaves, their wristband is read at the cash register, and the amount they owe tabulated. The display can alternatively be a diamond emitter display.

C. Utilities and metering - An apartment complex has  
15 large telephone wire boxes located outside which the telephone company services. The biometric patterns of authorized repair workers are stored by the telephone company. Access to the telephone box is denied to unauthorized people (who might surreptitiously activate their own telephone service). When an  
20 authorized repair worker wants to access a box to connect service for a new apartment dweller, he places his middle finger on the touch finger unit on the box, as shown in figure 124 and figure 124a. The finger unit's molded (slightly concave) acoustic transducer reads his middle finger boneprint biometric pattern and  
25 relays it by modem 197 to the telephone company. The telephone company computer 158 confirms authorization (in either identify or

verify mode) and by modem 197 causes a release mechanism to unlock the telephone box.

A homeowner builds a house with an electric meter in the utility room. The electric meter is equipped with a touch electrode card reader 174/determining mechanism 293, as shown in figure 125. Once a month, the homeowner grasps the card electrodes (nippled gold, 2 mm in diameter) and places it into the reader 174 (five frequencies and two waveforms). The homeowner's known pattern is stored separately in the house's centralized computer 158, with which the reader 174/ determining mechanism 293 communicates via microwave (2,450 MHZ) signals. The reader 174/determining mechanism 293 compares the present and known biometric patterns. Upon authorizing the homeowner by matching biometric patterns, the electric meter modems 197 data on the amount of electricity consumed to the electric company computer 158. The modem 197 also sends information to the homeowner's bank debit account and the money for the electricity bill is debited to the electric company. The meter resets to zero.

Another homeowner builds a house with an electric meter in the utility room. The electric meter is equipped with a touchless magnetic field hand sweep biometric device housing sensors 333, reader 174, determining mechanism 293, and memory all together, as shown in figure 126. The electric meter is equipped with a control panel on the front, with flip up arms containing the magnetic field sweep sensors 333. Once a month, the homeowner

flips open the sensor 333 arms at right angles to the control panel, and parallel to each other. The arms are activated in this position. The homeowner sweeps their hand through the magnetic field between the arms and the magnetic field hand sweep biometric  
5 device determines their present pattern and compares it to their known pattern for authorization. Upon authorizing the homeowner by matching biometric patterns, the electric meter modems 197 data on the amount of electricity consumed to the electric company computer  
158. The modem 197 also sends information to the homeowner's bank  
10 debit account and the money for the electricity bill is debited to the electric company. The meter resets to zero.

D. Mass transit and toll - As shown in figure 127, a business person takes the subway to work every day. The business person opens an account with the subway and is billed on a monthly  
15 basis. To use the subway, the business person places their hand on a touch hand unit, with 18 electrodes covering the palmar surface of the hand. It reads their biometric pattern using 12 frequencies. The pattern data is communicated to the subway computer 158, or by modem 197 to another subway computer 158, for  
20 comparison with the known biometric pattern on file (either identify or verify mode.) Matching the biometric pattern authorizes the business person to proceed onto the subway.

A commuter must take the toll turnpike to work. The toll booths are fitted with IR receivers 335, as shown in figure 128.

25 The commuter has a sensor 333/reader 174/determining mechanism 293

unit installed at the upper, driver's side, edge of the windshield. The sensor 333 unit is powered by the car's electrical system (battery). On the outside of the windshield, the sensor 333 unit has a small IR transmitter. Communicating with it on the inside of  
5 the windshield, the sensor 333 unit contains an acoustic touch thumb sensor 333, with red, green, and yellow lights. The red light means the sensor 333 is in standby. The green light means the sensor 333 has verified an authorized thumb boneprint and is transmitting an authentication and account information signal. The  
10 yellow light means only 5 seconds of transmission remain. A blinking yellow light means the boneprint verification was near selected confidence limits and the user should consider restoring the known biometric pattern to eliminate problems with pattern drift over time. The commuter has an account with the toll  
15 turnpike which is paid monthly by automatic credit card billing. Upon reaching a toll booth, the commuter presses their thumb against the thumb sensor 333 inside the windshield. Pressure activates the sensor 333, which obtains the present biometric pattern and compares it to the known biometric pattern stored in  
20 the microprocessor chip in the unit. The patterns match. The green light flashes and the IR transmitter transmits an authentication and account information signal, which is received by a receiver mounted in the toll aisle. The amount of the toll is billed to the consumer's account, the gate rises, and the commuter  
25 goes to work.

A business person rides the bus to work every day. The person pays for their bus fare with a stored value card in the form of a contactless smart card fitted with 1mm diameter touch electrodes in scalloped indentations on the card edges, as shown in figure 129. Upon entering the bus, the person grasps the card edges, finger and thumb flexion creases on the electrodes, and waves the card over the bus scanner. The scanner powers the card microprocessor 293 wirelessly, which compares the present and known biometric patterns 162. It transmits an authorization code to the scanner as well as account information 335. The bus scanner is powered by the bus battery.

E. Payphones - A traveler wishes to call home using a calling card. The touch calling card is fitted with a transducer and a memory with the known biometric pattern and account information, as shown in figure 130. The traveler inserts the transducer card into a unit on the telephone equipped with contact plate, reader 174, and determining mechanism 293. The unit takes the travelers' present biometric pattern, reads the memory 172 from the card, and compares the two. Upon verification, the traveler places the call home, and the account is billed for the call.

A traveler wishes to call home without using a calling card. The traveler grasps the biometric touch electrodes molded onto the curved surface of the telephone hand piece, dials their home phone number, and hits # # #, as shown in figure 131, figure 131a and figure 131b. The telephone hand piece sensors 333 are



connected by wires to a reader 174 and determining mechanism 293 inside the payphone, which obtain the travelers' present biometric pattern. The telephone communicates by modem 197 with a computer 158 for the traveler's area code, which stores known biometric patterns authorized for each phone number. The telephone compares the known and present biometric patterns to authorize the travelers' call, and the telephone number is billed for the call.

003064004000  
A traveler wishes to call home without using a calling card. The traveler dials their office phone number, and hits # #  
10 #. The side of the telephone box is equipped with a small touchless microwave field finger sweep unit, which obtains a biometric pattern based on interruption of the microwave field due to differing dielectric constants in unique tissue configurations in the finger, as shown in figure 132 and figure 132a. The unit  
15 contains sensor 333 (transmitter/receiver arms parallel to each other and at right angles to the side of the phone), reader 174, determining mechanism 293 and memory 162. Memory is updated by modem 197 every 8 hours. The traveler presses a button next to the finger sweep unit (activating the transmitter/receiver for 4  
20 seconds) and draws their index finger through the unit transmitter/receiver, between the parallel arms. The unit obtains the travelers' present biometric pattern and compares it to the known biometric patterns registered to the traveler's office phone number. The patterns match, the call is authorized, and the  
25 telephone number is billed for the call.

F. Healthcare and social services - A medical insurance company makes payments to hospitals and doctors electronically. Only certain people in the company are authorized to approve and initiate the electronic payments. The authorized payers place  
5 their hand on an electrode hand piece in the insurance company's financial office, as shown in figure 133. The biometric pattern data is communicated to the insurance company's computer 158, for comparison with the known biometric patterns 162 on file. This can be done in either identify or verify mode. Matching of the  
10 biometric pattern authorizes the payer to proceed with the electronic payments action 335.

A patient has a medical savings account (MSA). The patient also has a transducer card storing information on the MSA and the patient's biometric pattern, as shown in figure 188. The  
15 patient goes to the emergency room. To pay the bill, the patient inserts the MSA card into a reader and grasps the transducer. The reader verifies that the patient is authorized and initiates a transfer from the patient's MSA to the emergency room to pay the bill.

20 A patient has a medical savings account (MSA). The patient also has an electrode card storing information on the MSA and the patient's biometric pattern, as shown in figure 134. The patient goes to the emergency room. To pay the bill, the patient inserts the MSA card into a reader 174 and grasps the electrodes.  
25 The reader 174 verifies that the patient is authorized and

initiates a transfer from the patient's MSA to the emergency room to pay the bill.

A patient has a medical savings account (MSA). The patient also has a smart card storing information on the MSA and the patient's biometric patterns for several touch and touchless devices, as shown in figure 135. The patient goes to the emergency room. The emergency room uses a touchless sensor 333 of the type measuring electric currents in the fingertips upon sweeping the palm of the hand over an electric field power source. To pay the bill, the patient inserts the MSA card into a reader 174 and sweeps their hand over the sensor 333 device. The reader 174/determining mechanism 293 verifies that the patient is authorized and initiates a transfer from the patient's MSA to the emergency room to pay the bill. The hospital's reader 174 is plugged into the wall outlet, as shown in figure 188.

G. Wireless communications - A restaurant maintains accounts for its customers. A patron wishes to place a telephone call, while waiting for dinner. The waiter brings a portable telephone fitted with electrodes in the hand piece to the table, as shown in figure 136. The patron grasps the electrodes on the phone, which communicates with the restaurant computer 158 (housing memory, reader 174 and determining mechanism), either identifying or verifying the patron. The patron places the call and their restaurant account is billed for the call.

A lawyer uses a hand-held video phone equipped with a biometric sensor 333 to prevent unauthorized use and powered by rechargeable batteries. The biometric sensor 333 flips up from a recessed area on the side of the video phone, as shown in figure 5 138. It is round and flat, with a gold-plated electrode on each side (2 mm diameter, 0.5 mm thick). Authorization to use the video-phone is obtained by the lawyer flipping up the sensor 333 and grasping the electrodes sequentially between thumb and index finger, thumb and middle finger, and so on.

10 A lawyer uses a hand-held video phone equipped with an acoustic biometric sensor to prevent unauthorized use and powered by rechargeable batteries. The transducer is made of piezoelectric polymer molded onto the side of the video phone, on a pressure activated housing, as shown in figure 189. Authorization to use 15 the video-phone is obtained by the lawyer pressing on the transducer sensor with his index finger. The transducer reads his index finger boneprint and compares it to the boneprint on file.

Generally, the biometric system can be used on any type of stationary or portable communications device including, but not 20 limited to, cell phones and handheld phones.

H. Pay TV - Parents of teenaged boys install a lock-out system on the television, plugged into a wall outlet. The lock-out system contains an electrode hand piece and a mechanism to allow only authorized users to view adult channels, as shown in figures

138 and 138a. Only the parents are authorized users. When the teenagers attempt to access the adult channel, they cannot provide the correct biometric pattern and are unable to. The same is applicable to radios, as shown in figure 138b.

5           An army barracks has a rec room with a pay TV. The pay TV is fitted with an electrode card reader 174/determining mechanism 293 device, as shown in figure 139. When a soldier wishes to see a pay-per-view movie, an electrode military ID card is inserted into the device. When he grasps the electrodes on the  
10 card, the device compares the soldier's present biometric pattern to the pattern on the card, and to the pattern in the military base computer 158. The patterns match, the soldier is shown the movie, and the cost for the pay-per-view movie is deducted from the soldier's pay.

15           An army barracks has a rec room with a pay TV. The pay TV is fitted with a contact card device housing sensors 333, reader 174, and determining mechanism 293, as shown in figure 140. When a soldier wishes to see a pay-per-view movie, he inserts his military ID card into the card device. He then holds his hand over  
20 the touchless electric field sensor 333, of the type measuring induced currents simultaneously in all the fingers, upon holding the palm of the hand over the electric field source. The device compares the soldier's present biometric pattern to the pattern on the card, and to the pattern in the military base computer 158.

The patterns match, the soldier is shown the movie, and the cost for the pay-per-view movie is deducted from the soldier's pay.

An army barracks has a rec room with a pay TV. The pay TV is fitted with a transducer card reader/determining mechanism device, as shown in figure 190. When a soldier wishes to see a pay-per-view movie, their transducer military ID card is inserted into the device. When he grasps the transducer on the card, the device compares the soldier's present biometric pattern to the pattern on the card, and to the pattern in the military base computer. The patterns match, the soldier is shown the movie, and the cost for the pay-per-view movie is deducted from the soldier's pay.

I. Education - Educational institutions such as Florida State University use a card system. The card has items such as the student's color photo, signature, and university status in memory. The student uses the card for identification on campus; for physical access to dormitories, classrooms, buildings, libraries, and university offices; to check out books at the library; for banking on campus including a personal account, ATM withdrawals, payments for room and board, tuition payments, electronic purse, and pre-paid value for copiers and vending machines and such; for local merchant loyalty programs; to access personal University data; for telecommunications including local and long-distance calls from campus payphones; for bus passes; and for voice messaging. These and other functions can be performed more securely

and privately using a biometric signature linked to the student. This is done easily using any of the biometric sensor cards with memory. Other devices include hand pieces at various school locations, biometric sensor door handles, and the student's  
5 biometric sensor PC mouse or keyboard.

J. Travel - A business traveler makes frequently flights on FlyHigh Airlines. The airline places hand units at check-in stations for their frequent travelers, as shown in figure 141. The traveler places their hand on the hand unit, which reads the  
10 biometric pattern. The pattern data is communicated to the airline's hand unit computer 158, or by modem 197 to another airline computer 158, for comparison with the known biometric pattern on file. This can be done in either identify or verify mode. Matching of the biometric pattern authorizes the traveler's  
15 check-in to proceed electronically and instantaneously, as shown in figure 142. No more long lines.

A business traveler makes frequently flights on FlyHigh Airlines. The airline issues memory sticks to travelers, storing biometric and account information. The airline installs touchless  
20 "L" shaped hand units at check-in stations for their frequent travelers, as shown in figure 143. The hand unit has two surfaces, one horizontal surface parallel to the floor and housing electric field detectors, and another low vertical surface at right angles and facing away from the traveler and housing an electromagnetic  
25 transmitter. The traveler sweeps their hand over the horizontal

surface. An electric eye in the unit activates the electromagnetic transmitter, and the electric field detectors read the biometric pattern as sequential slices of data. The pattern data is communicated to the airline's hand unit computer 158, or by modem 5 197 to another airline computer 158, for comparison with the known biometric pattern in the memory stick (verify mode), as shown in figure 144. Matching of the biometric patterns authorizes the traveler's check-in to proceed electronically and instantaneously. No more long lines.

10 The business traveler must leave the country and go through customs. The traveler has an electronic passport containing their personal information and biometric signature, as shown in figure 145. The traveler places the electrode card into (contact) or near (contactless) a reader 174/determining mechanism 293 at 15 customs, grasping the electrodes. The reader 174 obtains the known biometric pattern and personal information from the card (verify mode) and the determining mechanism 293 compares it to the traveler's present biometric pattern. The patterns match and the traveler is cleared through customs in a matter of minutes.

20 The business traveler must leave the country and go through customs. The traveler has an electronic passport containing their personal information and biometric signature stored in a smart card. The traveler holds the scalloped edges of the smart card and holds it over a contactless touchless biometric device at 25 the customs exit, as shown in figure 146. The contactless



touchless device has a horizontal surface containing a radio transmitter for communicating with the microchip 189 in the underside of the smart card via the antenna 187. A low vertical surface facing away from the traveler houses a microwave transmitter, which emits microwaves at the travelers hand when activated. A second horizontal surface above the traveler's hand contains magnetic coils for detecting induced currents from the microwaves, which produce the biometric pattern. The device obtains the known biometric pattern and personal information from the card (verify mode) and compares it to the traveler's present biometric pattern. The patterns match and the traveler is cleared through customs in a matter of minutes.

K. Brokerages and equities - A brokerage firm allows on-line trading by its clients. Mobile clients can make trades using a lap-top PC and wireless technology, as shown in figures 147, 147a, 147b and 147c. Biometric authorization is provided by a small linear acoustic transducer (1mm x 12 mm) which flips up at right angles with the PC surface, from a flush recess. The client sweeps the palmar surface of their index finger from first crease to fingertip along the acoustic sensor 333. The boneprint signature matches that on file with the brokerage firm, and the client is authorized to complete the trade.

A brokerage firm allows on-line trading by its clients. Mobile clients can make trades using a lap-top PC and wireless technology, as shown in figures 148, 148a, 148b and 148c. The PC

has a small, spring loaded, fingertip-sized flap flush with its side. When the client presses in on the flap with their index finger an electromagnetic transmitter is activated, and it directs electromagnetic energy at the fingertip, parallel with the finger.

- 5 Electric field detectors in the flap measure the biometric pattern. The electric signature matches that on file with the brokerage firm, and the client is authorized to complete the trade.

II. Information technology - Successful development of an information society depends on trust between unseen partners.

- 10 These partners - customers, merchants, employers, banks, databases, governments, and the like - need to know that the identity claimed by the person at the other end is indeed genuine. Authentication of identity can then facilitate rightful access to information in any number of data storage systems and databases.

- 15 Three systems now in use attempt to meet this need: public key cryptography, digital certificates, and smart cards. Public key cryptography is a method of scrambling information by using two numbers, called keys, and complex mathematical operations to scramble and unscramble digital data. The "public" key is  
20 widely available, while the " private" key is available only to the authorized user of the key. Unfortunately, there is no reliable way to confirm that the person presenting a public key, is the authentic user of the matching private key.

Digital certificates were developed to solve this problem. Certificates are data files that contain a person's public key with other information such as the person's name and address, as well as the name and authorization code of the  
5 certification authority that issued the certificate.

The problem with digital certificates, is that anyone who gains access to the private key, through hacking or piracy, can assume the authorized person's identity and engage in fraudulent use of the certificate. Because the digital certificate does not  
10 absolutely link itself to a particular individual, it is like a passport without a photograph.

To solve this problem smart card applications were developed, incorporating public key cryptography and digital certificate methods. The private key is stored on the smart card,  
15 rather than on the PC hard drive. This protects the private key from piracy and hacking. The problem with smart cards is that private key authentication is linked to a particular card, rather than to a particular person. If stolen, the card can be used to gain unauthorized access.

20 Biometric linking of one person to the private key is an improvement on these systems. The biometric signature or its index is stored on the card or digital certificate. Presentation of the correct biometric signature is required to access the private key.

Even if the card or certificate is stolen, the thief cannot present the correct biometric signature to use it.

A. Loyalty and retail systems - Patrons of a retail chain are given points whenever a purchase is made. Points are redeemed for gifts chosen from the retailer's merchandise, as shown in figure 149. The points are stored on a microchip 189 card with biometric electrodes. The card, with its valuable accrued points, cannot be used by anyone other than the rightful owner. Payphones or cash registers at the point of sale (POS) are fitted with card readers 174. The customer places the electrode card into (contact) or near (contactless) the reader 174, grasping the electrodes, as shown in figures 150, 149. The biometric signature is communicated to the retailer's cash register computer 158, or by modem 197 to another computer 158, for comparison with the known biometric pattern on file. This can be done in either identify or verify mode. Matching of the biometric pattern authorizes the customer to redeem the valuable points.

At another store, the biometric pattern is determined using a touchless device measuring magnetic properties via reflected electromagnetic waves from the customer's hand, as shown in figure 151. The electromagnetic waves are of sufficient frequency, such as infrared or microwaves, to penetrate beneath the skin and obtain an internal biometric pattern. The customer does not even need to carry a card because their account information is located via identify mode. The customer simply places their hand

over a transmitter 333/receiver 174 on the cash register 293. Their account information appears on a screen 335 for their confirmation.

At another store, the biometric pattern is determined  
5 using an acoustic device measuring the acoustic properties of the bones in the customer's hand, as shown in figure 191. The customer simply places their hand on the acoustic hand piece near the cash register. They are identified by the acoustic handprint and their account information appears on a screen for their confirmation.

10 B. Government ID - Accurate, up-to-date, and portable information systems have been identified as being key to timely, fraud-proof delivery of government services. Smart cards are proposed for driver's licenses (Argentina and El Salvador already use them). The smart license can store "lasting" information  
15 (name, address, license #, citizenship, blood type, etc.) and "passing" information (driving record and outstanding fines). Traffic officers are equipped with either stationary readers 174 on their vehicles or hand-held readers 174 that can be carried to the traffic violator's vehicle, the way ticket books are carried now.  
20 The smart license can be fitted with sensors 333 such as electrodes, as shown in figure 152. The driver places the electrode license into (contact) or near (contactless) the reader 174, grasping the electrodes. The reader 174 obtains the biometric pattern from the card (verify mode) and authenticates the driver's  
25 claimed identity. The traffic offense is updated directly on the

smart license and by wireless modem 197 with the main traffic computer 158. Alternatively, the hand-held reader 174 can store all the traffic offenses for later down-loading to the traffic computer 158. Alternatively the smart license can contain a  
5 transducer or other sensor(s) rather than electrodes, to determine the biometric boneprint of the driver's thumb, as shown in figure 192.

The business traveler must leave the country and go through customs. The traveler has an electronic passport containing  
10 their personal information and biometric signature, as shown in figure 153. The traveler places the electrode card into (contact) or near (contactless) a reader 174 at customs, grasping the electrodes. The reader 174 obtains the known biometric pattern and personal information from the card (verify mode) and compares it to  
15 the traveler's present biometric pattern. The patterns match and the traveler is cleared through customs in a matter of minutes.

Access to computer 158 databases at the Central Intelligence Agency (CIA) is restricted. Access can be authorized and audited using biometric authentication, as shown in figure 154.  
20 A hand unit can be installed at doorways to computer 158 terminal rooms. The hand unit uses an acoustic field to produce direct currents in the biological semi-conductor structures of the applicant's hand. These structures are unique and produce biometric patterns for the hand. The hand unit consists of two parallel  
25 surfaces, the lower one consisting of a material producing an

acoustic field, and the upper surface housing electric field detectors. The person seeking access to the room places their hand on the lower plate. Their DC pattern is detected by the upper surface and compared to their biometric pattern on file.

5           Access to the most top-secret computer 158 databases at  
the (CIA) can be restricted and audited using a more secure  
biometric authentication. A hand unit can be installed at doorways  
to computer 158 terminal rooms, as shown in figure 155. The hand  
unit uses a multi-frequency acoustic field scan to produce  
10 alternating currents in the biological structures of the  
applicant's hand. These structures are unique and produce biometric  
patterns for the hand at each frequency, yielding accuracy greater  
than one in a billion. The hand unit consists of two parallel  
surfaces, the lower one consisting of a material producing an  
15 acoustic field, and the upper surface housing magnetic field  
detectors. The person seeking access to the room places their hand  
on the lower plate. Their AC patterns are detected by the upper  
surface magnetic field sensors and are compared to their biometric  
pattern on file.

20           C.     Identification - The biggest problems with  
identification papers and cards are fraud and copying. Use of a  
biometric signature and a micro-processor (complete with unique  
serial number, protected area, and cryptographic authentication) in  
a sensor 333 smart identification card prevent all but the most  
25 scientifically sophisticated abuses, as shown in figure 156.

Customers, merchants, employers, banks, databases, governments, and the like, can know with some assurance that the identity claimed by the person with the card is indeed genuine.

5 D. Time card systems - The first day on the job, a new employee is issued an electrode wristband. The wristband contains a contact plate 173 and an embedded microchip 189, as shown in figure 157. The microchip 189 contains data on the employee's biometric wrist signature, digital certificate, public and private keys, and level of access to physical and network facilities. When  
10 the employee arrives at work in the morning, they place the wristband in contact with a reader 174 on the wall next to the door. The contact plate 183 in the reader 174 communicates with the contact plate 173 on the wristband, reads the biometric signature and authorizes the employee to enter. The door unlocks.  
15 The time of the employee's arrival is archived for the time card system. The same sequence of events occurs when the employee leaves for the day. Similarly, the same system is used whenever the employee attempts to enter rooms or databases in the facility with limited access. The employee's successful entry into limited  
20 access areas is archived, as well as the employee's attempted entry into areas for which they are not authorized.

E. Healthcare - A hospital uses electronic medical records. The records are accessible on chart-sized portable PC notepads for use by hospital personnel. The notepads communicate  
25 with the various hospital department computers wirelessly. When a



nurse wishes to chart information on Mrs. Jones, the nurse activates a notepad, as shown in figures 158, 158a and 158b. Activation is accomplished by providing an authentic biometric signature, through electrodes on the rim of the notepad, in either  
5 identify or verify mode. The notepad, based on her authentication, authorizes her to read and write on the charts of only those patients for which she is providing care. Mrs. Jones is one of her patients, and the nurse is authorized to chart her care.

Another hospital uses electronic medical records and  
10 personal area networks (PANs) for its doctors. The records are accessible on chart-sized portable PC notepads for use by hospital personnel. Doctors are issued PAN wrist devices coordinating cellular phone, pager, personal digital assistant, and digital watch capabilities, as shown in figure 159. The wrist devices  
15 display data and communicate only after activation by the doctor's authentic biometric signature, through electrodes on the inside of the wristband, in a simple verify mode. Pages, phone calls, and access to patient care databases are authorized by the biometric wristband. To access an electronic medical record, the doctor  
20 holds their wristband near a computer 158 terminal. The wristband PAN and the computer 158 communicate wirelessly, the wristband authenticates the doctor's biometric pattern, and the computer 158 logs the doctor into the database. If a thief steals the doctor's watch and attempts to access the same patient care database, they  
25 will be unable to supply the correct biometric signature and will be unsuccessful.

Alternatively, the PAN wristband is fitted with two transducers of flexible piezoelectric polymer on either side of the wristband face. The transducers are thus positioned adjacent to the radius and ulna bone at the wrist. Unique biometric patterns  
5 are produced by the boneprints from these bones. The acoustic wristband functions as described above.

In addition to patient medical records, biometric signatures can also be used to access and record healthcare information by patients, third party payers, health care workers,  
10 and health care organizations, for managing administrative data such as verifying eligibility of individual claims and benefits, processing claims, obtaining pre-approval, risk management, quality improvement and error reduction, admission and discharge from facilities, and patient tracking within facilities. Use of  
15 biometric signatures with electronic medical records can protect patient privacy and health, by authorizing efficient and confidential sharing of information between authorized parties for the delivery and monitoring and payment of healthcare services.

F. Social Services - Biometric signatures can also be  
20 used to access and record social services information. A woman is eligible for Aid to Dependent Children, food stamps, and Medicaid. She is given an electrode card with microchip 189 memory, as shown in figure 160. When she seeks care at a physician's office, she presents the card which contains data on her Medicaid eligibility  
25 status, coverage type, and service limitations. She verifies that

she is the true authorized user of the card and services by providing a biometric signature, obtained through the card electrodes.

When the woman goes to the grocery store to buy food, she  
5 uses the card to pay for the food. She verifies that she is the  
authorized user of the card by providing a biometric signature via  
the card electrodes. The store reader 174 communicates by modem  
197 to the food stamp computer 158 and the woman's food stamp  
account for the month is debited. Alternatively, this can be done  
10 as either a credit account, or stored value card.

Alternatively, the sensor card contains a piezoelectric  
polymer which functions as an acoustic transducer, rather than  
electrodes, as shown in figure 193, to determine the biometric  
boneprint of the woman's thumb.

15 Use of biometric signatures for social services can  
provide eligibility verifications, allow high precision on  
benefits, restrict purchases to essential items, prevent fraud,  
improve efficiency, improve service delivery to truly needy  
beneficiaries, allow data tracking and surveys, and eliminate the  
20 need for monthly mailings.

G. Financial Transactions - Electronic commerce requires  
safe, portable, and simple systems which allow only authorized  
transactions. Businesses, financial institutions, and customers

alike need to know that the entity on the other end of the modem 197 is legitimate. For example, an on-line service provider, such as USA On-Line (UOL), can function as a secure electronic commerce authority. UOL would use encrypted keys and biometric signatures 5 to identify or verify the users. A customer would provide their biometric signature through sensors placed on their keyboard 128, mouse 126, lap-top frame, wristband, glove, card 170, internet phone, virtual screen glasses, or other device. The computer 158 servicing the merchant would be authorized daily, and after an 10 interruption of operations by a valid biometric signature.

For example, a customer desiring well controlled access to his private electronic records uses a biometric glove, as shown in figures 161, 161a and 161b. He wears the glove continuously while accessing his electronic records and biometric signatures are 15 assessed randomly and repeatedly throughout his access. The glove fits over the palm of his hand and over two-thirds of each finger, leaving the fingertip free. The palmar surface of the glove contains a multi-frequency magnetic field generating mechanism. The back surface of the glove contains sensors 333 for detecting 20 acoustic fields, in contact with the back of the hand and fingers. The multi-frequency magnetic field produces an acoustic pattern unique at each frequency, which serves as the biometric identifier. The glove communicates with a reader 174 unit in the device with which he accesses his electronic records.

To avoid repetitive typing of account information, consumers can store their account information on a simple electrode card. The customer simply inserts their electrode card into a reader 174 in or connected to their Internet device. Instead of  
5 entering a PIN code to unlock the card, the customer's own biometric signature serves as the code to unlock the card and authorize the transaction.

H. Software licensing - Software copying and piracy are significant problems for software developers. In spite of written  
10 licensing agreements, purchasers of software are often able to give copies to friends and associates. Schemes that make the software computer-specific, deprive the purchaser of the ability to rightfully move the software to a new computer 158. Consequently, software merchants lose a great deal of income from unauthorized  
15 copying of their programs. Biometric signatures can eliminate this problem and allow software merchants to sell user-specific software, as shown in figure 108. The software is written to run only after an authorized biometric signature is entered via sensor 335 mouse, keyboard, card, hand piece, joystick, or other such  
20 device. When the computer 158 is turned on and the system and programs booted, the authorized biometric signature is required to initiate the software. The software can also require re-entry of an authorized biometric signature, for instance, every 4 hours, to prevent defeat of the user-specific requirement by leaving the  
25 computer 158 running continuously. When the authorized user buys

a new computer 158, the software can be loaded on to the new one by reloading the biometric signature.

For instance, Windows 2005 can require biometric authentication to function properly. The authentication is  
5 obtained by a sensor 333 recessed in the mouse employing electromagnetic transmission to the index finger, leading in turn to an acousto-electric effect detected via an acoustic sensor 333 pad. On a right handed mouse, the left button cover flips up at a 45 degree angle revealing the sensor 333 assembly, as shown in  
10 figures 162a, 162b and 162c. The lid contains an antenna for transmitting electromagnetic energy. The bottom, palmar surface of the sensor 333 assembly, inside the mouse, contains a piezoelectric polymer molded slightly concavely to fit the index finger comfortably. The sensor 333 assembly is pressure activate. To  
15 operate, the user flips up the button cover and slides their index finger in, touching against the bottom surface. By clicking the assembly with their index finger, the biometric scanner is activated and their biometric pattern is read and compared to that on file within the Windows 2005 operating system.

20 Alternatively, the mouse contains either simple electrodes to obtain an electric/magnetic biometric signature, or a transducer placed under the thumb or fingers to obtain a boneprint biometric signature, as shown in figure 194. A biometric system with electrodes or a transducer placed on a "smart quill"

type pen, such as that offered by British Telecom Labs in Ipswich, England, can be used to control usage and operation of such a pen.

III. Access control systems - Access control systems involve access to three main things - physical areas, physical objects, and virtual areas. Physical areas include real estate and installations such as homes, offices, apartments, hospitals, factories, military bases, stores, prisons, rooms, hallways, and such. Physical objects include personal property, both tangible and intangible, such as water craft, aircraft, land vehicles, weapons, cabinets, furniture, appliances, tools, computer hardware, briefcases, documents and files representing intangible personal property, and such. Virtual areas include all manner of intangible personal property, computer software, and electronic data systems, with their databases, information, and communication systems.

Customarily, access to areas and objects is controlled using locks. Locks traditionally are operated by any number of mechanisms including keys, timers, combinations, passwords, numbers, or electronically. Lock operation is linked to a particular mechanism, rather than a particular person.

Biometric locks are linked to a particular person. Biometric locks are operated by the correct biometric pattern, rather than by a traditional lock operating mechanism such as a key or code. A biometric lock can be discrete, composite,

multiple, or optional. Discrete biometric locks 211 use the biometric pattern to totally replace the traditional lock 211 operating mechanism (such as a key or code). In the discrete biometric lock 211, the biometric pattern is the only mechanism  
5 operating the lock 211. An example of a discrete biometric lock 211 is a door handle containing biometric electrodes which unlock the door, only when an authorized person places their hand on the door handle electrodes and provides their biometric impedance pattern, as shown in figures 163, 163a, 163b, 163c and 163d, the  
10 latter being a car door type handle. Similarly, handles with acoustic transducers are shown in figures 163e, 163f, 163g and 163h.

A composite biometric lock 211 requires both a biometric pattern and a traditional lock 211 operating mechanism, as shown in  
15 figure 164. An example of a composite biometric lock 211 is a door handle containing biometric electrodes and a numerical keypad. The lock 211 opens only after the correct numerical code is keyed in AND an authorized person places their hand on the door handle electrodes and provides their biometric impedance pattern.

20 A multiple biometric lock 211 requires two or more biometric patterns to operate the lock 211. An example of a multiple biometric lock 211 is a door handle containing biometric electrodes and an acoustic boneprint scanner, as shown in figure 165. The lock 211 opens only after an authorized person places  
25 their hand on the door handle sensors 333 and their thumb on the



thumb flap, and simultaneously provides their electric finger AND acoustic boneprint biometric patterns.

An optional biometric lock 211 requires successful use of at least one, of two or more lock operating mechanisms (one or more of which is biometric). An example of an optional composite biometric lock 211 is a door handle containing biometric electrodes and a keyhole, as shown in figure 166. The lock 211 opens after an authorized person either opens the lock 211 with a metal key, or places their hand on the door handle electrodes and provides their biometric patterns. An example of an optional multiple biometric lock 211 is a door handle containing biometric electrodes and a boneprint scanner, as shown in figure 167. The lock 211 opens after an authorized person either places their hand on the door handle electrodes and provides their electric biometric patterns, or places their thumb on the boneprint scanner and provides their biometric boneprint pattern.

Lastly, a composite multiple biometric lock 211 is considered. This lock 211 contains at least one traditional lock operating mechanism, as shown in figure 168. It also contains two or more biometric lock 211 operating mechanisms. An example of a composite multiple biometric lock 211 is a door handle containing biometric electrodes, a boneprint scanner, and a keyhole. The keyhole is accessible only after an authorized person places their hand on the door handle sensors 333 and simultaneously provides their electrical and boneprint biometric patterns. Alternatively,

the composite multiple biometric lock can be optional. For instance, the keyhole can be accessible after an authorized person either places their hand on the transducers, and provides at least one valid biometric pattern.

5           A. Closed environments - Closed environments are simply those areas or objects which are not openly available to everyone. Preferably, the action is accessing an area as shown in figure 92, and the allowing mechanism includes a mechanism for allowing access to the area. The allowing mechanism preferably includes a lock 211  
10 and a release mechanism 215 connected to the recognizing mechanism 135 and the lock 211. The recognizing mechanism 135 produces a recognizing signal when the individual is recognized which is received by the release mechanism 215 and causes the release mechanism 215 to open the lock 211.

15           For instance, and referring to figure 92, in an area where there is controlled access, for instance by a door or a window into a room, or a gate into a fenced field, or a safe, there is some form of a lock 211, whatever that lock 211 may be, which prevents the door or the window or the gate to open when it is  
20 locked, as is well known in the art. By introducing the mechanism for recognizing a biometric signature of an individual, any one of which are described herein, and a release mechanism 215 connected to the recognizing mechanism 135 and the lock 211, access to the area is controlled. The biometric signature is used for  
25 recognizing the individual by the recognizing mechanism 135 which

causes a recognizing signal to be sent to the release mechanism 215. The release mechanism 215 can be some type of a motor which moves the lock 211, or simply an electric current that flows through a coil that creates a magnetic field which causes a lock 5 211 to open. Basically, any type of release mechanism 215 in conjunction with a lock 211, as is well known in the art can be used. Such a combination is simply connected with the recognizing mechanism 135, which serves as the controller for determining when the release mechanism 215 should operate.

10 For instance, a defense contractor wishes to restrict access to certain laboratories. Electronic locks 211 are installed on the doors to the laboratories, as shown in figure 169. To enter, an authorized laboratory technician places his hand in the hand unit installed on the wall next to the door. The hand unit 15 has two parallel surfaces - one against the wall and another five inches away from the wall. The surface against the wall contains acoustic field sensors 333, while the surface five inches away from the wall contains multi-frequency magnetic field transmitters. The technician places their hand on the acoustic field sensors 333 and 20 presses gently to activate the sensor 333/reader 174 device. Magnetic field transmitters utilize the acousto-electric effect to produce unique acoustic patterns at different frequencies, thereby producing a biometric signature. The sensor 333/reader 174 relays it by modem 197 to the laboratory computer 158. The laboratory 25 computer 158 confirms authorization (in either identify or verify mode) and by modem 197 causes a release mechanism to unlock the

door. The laboratory computer 158 also records the date, time, and identity of the technician entering the lab.

An office area in the defense contractor's facility is open to all employees. While no employees are restricted in their access, the company does want to know who enters the office. When an employee wishes to enter the office, they grasp the door handle, making contact with the biometric electrodes, as shown in figures 170 and 170a. The door handle is a curved vertical handle, with a thumb flap positioned above it on the door. It is normally operated by grasping the curved portion with the fingers, and pressing down on the thumb flap with the thumb. The electrode door handle is fitted with electrodes (tetrapolar, 1 mm diameter, nipped and molded with the handle surface) in the thumb flap for the thumb, and on the curved portion for the fingertips. Current is generated at the thumb and read at the fingertip electrodes. The biometric signature is identified, the door unlocks admitting the employee, and the company database records the date, time, and identity of the employee entering the office. In an alternate preferred embodiment as shown in figure 93, the area is a database and the allowing mechanism includes a mechanism 217 for allowing access to data in the database connected to the recognizing mechanism 135. The recognizing mechanism 135 producing a recognizing signal when the individual is recognized which is received by the allowing access mechanism and causes the allowing access mechanism to allow the individual to access the data base.

The allowing access mechanism preferably includes a computer 158, a memory 172 and an access program stored in the memory.

Similarly, as shown in figure 93, the area can be a data base having data stored in it. The data base can be connected with  
5 a computer 158 having a memory 172 and a program stored in the memory 172 which, when activated, the program causes the computer 158 to be able to access the data in the data base. The program would be activated by the recognizing mechanism 135 recognizing an individual through the individual's biometric signature and the  
10 recognizing mechanism 135 producing a recognizing signal which is provided to the computer 158 and which is received and processed by the computer 158 with the program. The program, upon receiving the recognizing signal, is activated, causing the computer 158 to be able to access the data base. In this case, the biometric  
15 signature is the substitute for a password that has to be entered into the computer 158. The well-known techniques of using a password for access to databases or other aspects of the computer 158 would be exactly the same except that the signal in which the password is provided to the computer 158 now becomes the  
20 recognizing signal from the recognizing mechanism 135.

A computer 158 database in the defense contractor's facility is accessed on a need to know basis only. Each employee is given access to various portions of the computer 158 system, based on their work. When an employee logs on, their biometric  
25 signature is authenticated. When an employee attempts to access a

restricted database, their biometric signature is again required. Access to a restricted database requires a second biometric signature via an electric field/acoustic hand piece, as shown in figures 171, 171a and 171b. The hand piece is a shell device which  
5 fits on the side of the monitor. The inside surface closest to the monitor has an acoustic field receiver such as a piezoelectric ceramic or polymer sheet. The outside of the shell, furthest away from the monitor contains a set of capacitors for generating an electric field. To access the restricted database, the employee  
10 slides their hand into the shell, placing the palm of their hand against the side of the monitor (against the piezoelectric surface.) A barrier between the capacitors and the piezoelectric surface prevents contact between the person's hand and the capacitors. The employee presses gently against the acoustic  
15 sensor 333, activating the electric field. The electric field is converted in the hand via the acousto-electric effect into a unique acoustic field pattern, which serves as the biometric signature. Alternatively, the sensor is a sole acoustic hand piece mounted on the side of the monitor, which provides an acoustic print of the  
20 employee's hand.

B. Security - A homeowner has biometric sensor door handles installed on the home's doors. When the homeowner wishes to enter the home, they grasp the door handle, making contact with the biometric sensors 333. The correct biometric signature is  
25 identified or verified and the door unlocks, admitting the homeowner.

The homeowner also has a cabin in the mountains, without electricity. The cabin is protected by a similar electrode door handle system, that is powered by mechanically produced electricity. In one embodiment, the homeowner turns a handle crank  
5 to charge a capacitor, as is well known by those skilled in the art for powering portable radios and telephones. In another embodiment, a handle winds a large spring, as in the Baylis generator, producing electricity to power the biometric door lock 211, as shown in figure 172.

10 The homeowner also owns a defensive weapon, to encase an intruder in a sticky goo that limits the intruder's movement. See U.S. Patent Application serial number 09/183,923, incorporated by reference herein. The homeowner does not want a would be assailant to use the homeowner's own weapon on the homeowner. The goo weapon  
15 handle is fitted with electrodes (tetrapolar, 1 mm diameter, nipped and molded with the handle surface) for the thumb, and third, fourth, and fifth fingers; or a thumb transducer, as shown in figure 173. Identification or verification of the homeowner's authorized biometric signature is required to activate the goo  
20 weapon. Alternatively, the sensor can be a transducer on the weapon handle.

A large military facility restricts vehicular access to areas, using guards and checkpoints. Those with authorization to travel in the facility are given touch electrode wristbands with a  
25 contact electrode, as shown in figure 174. When the vehicle

approaches the checkpoint, the occupants hold out the wristband and the guard places it in contact with a portable contact device (reader 174/determining mechanism 293/memory). An authorized biometric signature is obtained from the wrist electrodes, communicated via the contact electrode to the reader 174 device, and the vehicle is allowed to proceed.

C. Healthcare and social services - Access to the controlled substances storage cabinet in a hospital pharmacy is restricted to a small group of pharmacists. The cabinet contains a hand piece, as shown in figure 175. When an authorized pharmacist needs to add or remove controlled drugs, they place their hand on the hand piece, making contact with the electrodes. Their present biometric signature is identified from the small list of authorized users' known signatures, and the cabinet unlocks. The cabinet microprocessor records the date, time, and identity of the pharmacist entering the cabinet.

In another hospital, access to the controlled substances storage cabinet in a hospital pharmacy is controlled by biometric PAN cards, as shown in figure 176. The cabinet lock communicates wirelessly with the biometric PAN card. When an authorized pharmacist needs to add or remove controlled drugs, they hold the PAN card on the edge electrodes, and hold it up to the cabinet. The PAN card transmits with a transmitter 229 their biometric signature to the receiver 223 of the cabinet lock 211. Their present biometric signature is identified from the small list



of authorized users' known signatures, and the cabinet unlocks. The cabinet microprocessor records the date, time, and identity of the pharmacist entering the cabinet.

Electronic records are used in a large nursing home.

5 Doctors access the records using a forehead mounted headset fitted with virtual screen glasses in "see through" mode, as shown in figures 177, 177a and 177b. This allows the doctor to examine and talk to the patient while simultaneously seeing the patient records. Access to the patient record database is granted by  
10 biometric signature recognition in the form of a biometric signature of the forehead. This can be accomplished with electrodes or with an acoustic transducer positioned on the inner surface of the headset in contact with the forehead. The virtual screen glasses utilize a PAN system to communicate with the central  
15 records computer 158. The central records computer 158 also stores the known biometric patterns of the doctors.

D. Information technology - A telecommunications company maintains a computerized switching system. Physical components are periodically added to and maintained in the system hardware.  
20 Access to the hardware is biometrically restricted to authorized individuals. This is accomplished with electromagnetically induced currents, as shown in figures 178 and 178a. The authorized individuals are issued contactless smart cards, with electrodes in scalloped areas on the card edges. The individual holds the smart  
25 card on the scalloped edges, over the antenna/coupler unit on the

outside of the hardware. The antenna/coupler unit transmits electromagnetic energy wirelessly to the antenna in the smart card. The hand also acts as an antenna, producing induced currents which are read by the electrodes in the scalloped edges, producing a  
5 biometric signature.

A homeowner has a flat-screen portable TV, and a portable radio, both of which are powered by electricity generated from stored human mechanical energy. The mechanical energy can also be obtained from a small dynamic device powered by means of a crank.  
10 Biometric locks 211 on the devices via acoustic boneprints restrict use to authorized users only, as shown in figure 179.

E. Financial Transactions - ATM machines must be periodically emptied of banking documents and refilled with cash. Access to the machines is limited to the bank employees servicing  
15 the machines. Rightful limited access can be further assured by using biometric locks 211 on the ATM machines. Each ATM worker carries a transducer card, as shown in figure 180. To unlock the ATM, the worker inserts the transducer card into the reader 174 on the ATM, and presses their thumb on the transducer pad. The ATM  
20 reader 174 communicates by modem 197 with the bank computer 158, which identifies the worker from a small list of authorized workers and unlocks the machine. The date, time, ATM location, and identity of the ATM worker is recorded.

The bank learns that the ATM worker concealed their true identity and is actually a convicted felon. The ATM worker's authorization is immediately removed from the list of authorized workers. The ATM worker is ordered to return their transducer card  
5 to the bank. The ATM worker attempts to open an ATM to steal the contents. The ATM identifies the worker, keeps the ATM locked, and calls the police and the bank with the worker's location.

Alternatively, each ATM worker carries an electrode card, as shown in figure 195, which functions similarly in relation to  
10 the ATM as the transducer card.

F. Vehicles - The door handles and steering wheel of a land, water, or air craft are fitted with electrodes (1 mm diameter, tetrapolar) . The doors will not unlock until the biometric pattern of an authorized user is entered via the door  
15 handle, as shown in figures 181, 182, 182a and 182b. Similarly, entry of the authorized biometric signature via the steering wheel allows the vehicle motor to start. Automobile drivers no longer need to carry car keys to unlock the car or start the engine. The car will not unlock and the electrical system will not function for  
20 a thief, but rather only for the rightful owner.

The metal key to a vehicle contains an acoustic pad on the bow or head. When the key is inserted in the ignition, the metal tip on the key conducts current from the dashboard reader 174, to obtain the boneprint of the driver's thumb, as shown in

figures 183, 183a and 183b. The driver is identified and the ignition is unlocked. Based on the driver's profile, driving characteristics are controlled such as maximum speed, and access to adult establishments via a global positioning system.

- 5           G. Remotely operated devices - Numerous devices are operated by remote control such as vehicle ignition starters, vehicles unlocking devices, televisions, radios, garage doors, and the like. The remote control unit can be fitted with sensors 333 such as electrodes or transducer, as shown in figure 187.
- 10 Verification of an authorized biometric signature is required to operate the remote control.

#### IV. Electronic Tagging Systems

- A. House arrest - A convicted felon is sentenced to house arrest. The felon wears an ankleband fitted with biometric electrodes, as shown in figure 197. The ankleband communicates wirelessly with an antenna/coupler device connected to the felon's telephone, which communicates by modem 197 with a law enforcement computer 158. The biometric ankleband periodically communicates the felon's biometric pattern via the antenna coupler and modem 197
- 15
- 20 to the authorities, thereby confirming that the felon remains under house arrest.

Alternatively, the felon wears a transducer ankleband, with transducers positioned laterally over the distal tibia and fibula bones.

B. Locator - Crew members on a ship wear wristbands  
5 fitted with biometric electrodes inside the wristband. Each crew member's wristband is uniquely coded for wireless communications with the ship's computer 158 system, which allows the computer 158 to identify each crew member by their unique code. The captain of the ship can locate any member of the crew by activating a search  
10 mechanism with the ship's computer 158, as shown in figure 185. The crew member's name is input into the search mechanism and the unique communication code for that crew member's wristband is broadcast throughout the ship, as shown in figures 185a, 185b, 185c regarding acoustic signals, and figures 185d, 185e, and 185f  
15 regarding electrodes. Upon receiving the unique code, the wristband will assess the biometric pattern of the wearer and will respond in one of four ways: 1) The appropriate crew member is located; 2) No one is wearing the wristband; 3) a different crew member is wearing the wristband and is identified as Joe Smith by  
20 their pattern on file; 4) an unknown entity is wearing the wristband. When the wristband responds to the unique communication code, the location of the receiving antenna/coupler is determined. Detection of signal in multiple antenna/couplers combined with signal strength determination allows triangulation of the crew  
25 member's exact location.

A geologist for a petroleum company has a contactless PAN touch sensor 333 card which couples with the antenna/coupler unit in her company vehicle. The coupler unit also contains a transmitter/receiver unit for communicating with the global positioning system (GPS), as shown in figure 186. When the geologist transmits reports from the field her exact location can be ascertained via the GPS, and the validity of the report by her biometric signature.

The sensor card may contain electrodes for obtaining an electric/magnetic biometric signature, or transducer(s) for obtaining acoustic biometric signature, as shown in figure 196. A GPS on the wrist band, such as Casio's GPS, can also be present and activated with a biometric signature as explained above. The biometric system can be used with anything worn or attached, such as rings or jewelry.

A preferred embodiment of a hand piece unit is described as follows. A laptop computer (the Armada 7800 by Compaq) was programmed with LabView 5.0 (a graphical development program by National Instruments). The computer connected to a laptop docking station (the Armada Station by Compaq). Inside the docking station, a voltage source and data acquisition board was installed (multi-input/output PCI-MIO-16E-1 by National Instruments). The board specs: two analog output channels with 0.1 Ohm output impedance up to a current limit of 5 mA, range of -10 V to +10 V; 16 single ended analog input channels or 8 differential analog

input channels with input impedances of 100 Gohms, 12 bit resolution (1 in 4096), and sampling rates of 1.25 million samples per second; two 8 channel multiplexors; a programmable gain instrumentation amplifier with gains up to 100; 8 digital  
5 input-output lines.

The docking station connected via a 68-pin cable to an external electronics box and hand piece unit. The electronics box was made from a bread board and terminal block (National Instruments). The circuit on the bread board is shown in figure  
10 198. The digital lines and onboard power were used to operate transistors and relay switches to control measurement of individual current paths and to switch between two-terminal and four-terminal measurements. The unit provided one current generating point at the heel of the palm, and measurements were made on each digit of  
15 the hand. The driver frequency varied in a range was 100 Hz to 100 KHz. Measurements could be made for any combination of discrete frequencies and frequency ranges. A 9-in connector on the external electronics box allowed different electrode pieces to be connected.

The hand piece surface was placed in parallel over the  
20 breadboard and was constructed of a sheet of polycarbonate plastic (by Lexan). The electrodes were gold-plated stainless steel screws inserted up through the polycarbonate sheet. Standard copper wire connected the receiving electrodes to the circuit. A coaxial cable connected the current generating electrode to the circuit. The

hand piece surface was shielded from the bread board circuit with copper tape placed on the underside of the polycarbonate plastic.

Operational control and data analysis was performed by the laptop computer. Different sine waveform frequencies were generated using software programming of the multi-I/O board via digital synthesis. The user interface performed five functions: Master Pattern, Identify, Verify, settings and View Pattern. The Master Pattern scanned the resistance of the digits of the subject over a core set of frequencies and fingers as defined by the system operator and recorded the pattern of the subject in a database. Patterns were placed in one of 122 categories, depending on which digit had the highest resistance. The Identify function measured the resistance of the digits of the subject and compared the result to the previously recorded patterns to determine the best match. Rather than searching the entire pattern database for a match, only the patterns in the same master category were analyzed. The Verify function measured the resistance of the digits of the subject and compared the result to a previously recorded pattern for the subject. The Settings function allowed the user to modify various parameters of the pattern measurement such as constant current vs. constant voltage, two terminal vs. four terminal, and frequencies. The View Pattern function allowed the user to browse previously recorded patterns in a graphical display with the option to print the patterns.



**EXAMPLE**

Electronic Ink

A traveler wishes to use a biometric stored value card to pay for items while on vacation. They obtain a \$500.00 biometric stored value card from the bank. The value of the card is displayed on the outside of the card using E-ink (electronic ink). When the traveler uses the card to purchase an item, money credits are removed from the card. Say for instance that the traveler buys a meal for \$10.00. The card is inserted into a reader to read the traveler's biometric signature via the contact electrode on the card. The microchip within the card contains an address grid connected to conductive ink or other conductive material, which is connected to the E-ink display. The card removes \$10.00 credit and transfers it to the merchant. The E-ink display on the card is changed to read \$40.00 by sending a message from the microchip through the conductive material to the E-ink display.

In the alternative, the E-ink display can be with another card including but not limited to a credit, debit, ID, access, or PAN card. In the alternative, the E-ink display can be disposed on or in another biometric device including but not limited to a time card, a vehicle, a meter, a transit booth, a telephone, a TV, a cash register, a lock, a remote controller, an electronic tag, a locator, a positioning device, a wristband, a watch, a PAN system,

a memory stick, a computer, a video phone, virtual screen glasses, a handle, a weapon, a door, a gate, a handpiece, a computer.

The present invention pertains to a method for charging a purchase. The method comprises the steps of recognizing a  
5 biometric signature of a purchaser. Then there is the step of charging an account of the purchaser with the purchase price.

Preferably, the recognizing step includes the steps of obtaining a present biometric signature from a purchaser, and comparing a known biometric signature of the purchaser with the  
10 present biometric signature of the purchaser.

The obtaining step preferably includes the step of placing the hand of the purchaser in contact with a hand unit to obtain the biometric signature of the purchaser.

The present invention pertains to a method for charging  
15 a purchase. The method comprises the steps of recognizing a biometric signature of a purchaser using a sensor mechanism with unique characteristics. Then there is the step of charging an account of the purchaser with the purchase price.

The present invention pertains to a method for charging  
20 a purchase. The method comprises the steps of recognizing a biometric signature of a purchaser using a sensor mechanism sensing

acoustic characteristics. Then there is the step of charging an account of the purchaser with the purchase price.

5 The present invention pertains to a method for charging a purchase. The method comprises the steps of recognizing a biometric signature of a purchaser using a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of charging an account of the purchaser with the purchase price.

10 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching sensors 333 of a card 170 by the individual to generate a biometric signature of the individual. Then there is the step of reading the card 170 with a reader 174 and recognizing the individual from the biometric signature.

15 Preferably, after the touching step, there is the step of providing a present biometric signature from the card 170 to the reader 174, and comparing via the reader 174 the present biometric signature with a known biometric signature to recognize the individual.

20 The card 170 preferably includes a first side and a second side, and wherein the sensors 333 includes finger sensors 333 disposed on the first side and/or sensors 333 disposed on the second side and the touching step includes the step of touching

with at least one finger at least one finger sensor and touching with the thumb the sensor on the second side.

Preferably, the reading step includes the step of contacting a reader contact plate with a contact electrode 173 of the card 170 through which the present biometric signature transfers from the card 170 to the reader 174.

The contacting step preferably includes the step of inserting the card 170 in a groove of the reader 174 for the contact electrode 173 to contact the reader contact plate.

Preferably, the card 170 includes a credit card, debit card, stored value card, ID card, access card smart card or PAN card.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a card 170 having sensors 333 with a unique characteristic by the individual to generate a biometric signature. Then there is the step of reading the card 170 with a reader 174 and recognizing the individual from the biometric signature.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a card 170 having sensors 333 for sensing acoustic characteristics by the individual to generate a biometric

signature. Then there is the step of reading the card 170 with a reader 174 and recognizing the individual from the biometric signature.

5 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a card 170 having sensors 333 for sensing an electric and/or magnetic characteristic by the individual to generate a biometric signature. Then there is the step of reading the card 170 with a reader 174 and recognizing the individual from the  
10 biometric signature.

15 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching sensors 333 of a memory stick by the individual to generate a biometric signature of the individual. Then there is the step of reading the memory stick with a reader 174 and recognizing the individual from the biometric signature.

20 Preferably, after the touching step, there is the step of providing a present biometric signature from the memory stick to the reader 174, and comparing via the reader 174 the present biometric signature with a known biometric signature to recognize the individual.

The memory stick preferably includes sensors 333 and the touching step includes the step of touching with at least one finger one sensor and touching with the thumb another sensor.

5 The present invention pertains to a method for authorizing an action. The method comprises the steps of placing a memory stick in which is stored a known biometric signature of the individual into a memory stick reader 174 connected to a recognizing mechanism. Then there is the step of reading the biometric signature of the individual. Next there is the step of  
10 comparing it to the known biometric signature of the individual from the memory stick with the recognizing mechanism to recognize the biometric signature of the individual. Then there is the step of recognizing a biometric signature of an individual. Next there is the step of allowing the action when the recognizing mechanism  
15 recognizes the biometric signature of the individual.

Preferably, the reading step includes the step of touching by the individual sensors 333 of the recognizing mechanism to obtain the biometric signature of the individual. The reading step preferably includes the step of touching by the individual  
20 sensors 333 of the memory stick to obtain the biometric signature of the individual.

The present invention pertains to a method for authorizing an action. The method comprises the steps of placing a memory stick in which is stored a known biometric signature of

the individual of the individual into a memory stick reader 174  
connected to a recognizing mechanism. Then there is the step of  
reading the biometric signature of the individual having a sensor  
mechanism with unique characteristics. Next there is the step of  
5 comparing it to the known biometric signature of the individual  
from the memory stick with the recognizing mechanism to recognize  
the biometric signature of the individual. Then there is the step  
of recognizing a biometric signature of an individual. Next there  
is the step of allowing the action when the recognizing mechanism  
10 recognizes the biometric signature of the individual.

The present invention pertains to a method for  
authorizing an action. The method comprises the steps of placing  
a memory stick in which is stored a known biometric signature of  
the individual of the individual into a memory stick reader 174  
15 connected to a recognizing mechanism. Then there is the step of  
reading the biometric signature of the individual with a sensor  
mechanism for sensing an acoustic characteristic. Next there is  
the step of comparing it to the known biometric signature of the  
individual from the memory stick with the recognizing mechanism to  
20 recognize the biometric signature of the individual. Then there is  
the step of recognizing a biometric signature of an individual.  
Next there is the step of allowing the action when the recognizing  
mechanism recognizes the biometric signature of the individual.

The present invention pertains to a method for  
25 authorizing an action. The method comprises the steps of placing

a memory stick in which is stored a known biometric signature of the individual into a memory stick reader 174 connected to a recognizing mechanism. Then there is the step of reading the biometric signature of the individual with a sensor mechanism for  
5 sensing an electric and/or magnetic characteristic. Next there is the step of comparing it to the known biometric signature of the individual from the memory stick with the recognizing mechanism to recognize the biometric signature of the individual. Then there is the step of recognizing a biometric signature of an individual.  
10 Next there is the step of allowing the action when the recognizing mechanism recognizes the biometric signature of the individual.

The present invention pertains to a method for accessing an area. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique  
15 characteristic. Then there is the step of allowing access to the area when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing an area. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an  
20 acoustic characteristic. Then there is the step of allowing access to the area when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing an area. The method comprises the steps of recognizing a biometric



signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of allowing access to the area when the biometric signature of the individual is recognized.

5            Preferably, the area includes a lock and a release mechanism connected to the recognizing mechanism and the lock, wherein the recognizing step includes the step of producing a recognizing signal when the individual is recognized. Then there is the step of allowing step includes the step of receiving the  
10 recognizing signal by a release mechanism and causing the release mechanism to open a lock.

            The present invention pertains to a method for accessing a database. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of  
15 producing a recognizing signal when the individual is recognized. Next there is the step of receiving by an allowing access mechanism the recognizing signal which causes the allowing access mechanism to allow the individual to access part or all of the database.

            The present invention pertains to a method for accessing  
20 a database. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of producing a recognizing signal when the individual is recognized. Next there is the step of receiving by an allowing access mechanism the

recognizing signal which causes the allowing access mechanism to allow the individual to access part or all of the database.

5 The present invention pertains to a method for accessing a database. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of producing a recognizing signal when the individual is recognized. Next there is the step of receiving by an allowing access mechanism the recognizing signal which causes the allowing access mechanism  
10 to allow the individual to access part or all of the database.

15 The present invention pertains to a method for accessing a database. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of producing a recognizing signal when the individual is recognized. Next there is the step of receiving by an allowing access mechanism the recognizing signal which causes the allowing access mechanism to allow the individual to access part or all of the database.

20 The present invention pertains to a method for authorizing a financial transaction. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is

the step of allowing the financial transaction when the biometric signature of the individual is recognized.

The present invention pertains to a method for authorizing a financial transaction between a first account and a  
5 second account. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an acoustic characteristic. Then there is the step of allowing the financial transaction when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for authorizing a financial transaction between a first account and a second account. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is  
15 the step of allowing the financial transaction when the biometric signature of the individual is recognized.

Preferably, the allowing step includes the step of allowing a transfer of value between the first account and the second account. The allowing step preferably includes the step of  
20 allowing a transfer of money between the first account and the second account. Preferably, the allowing step includes the step of allowing a transfer of equities between the first account and the second account.

The present invention pertains to a method for gambling. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of placing a bet by the individual when the biometric signature of the individual is  
5 recognized.

Preferably, the placing step includes the step of placing the bet over a telecommunication line to a gambling mechanism. The step of placing the bet over a telecommunication line preferably includes the step of placing the bet via a telephone line, cable  
10 line or wireless connection.

The present invention pertains to a method for gambling. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism having a unique characteristic. Then there is the step of placing a bet by the  
15 individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for gambling. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism for sensing an acoustic  
20 characteristic. Then there is the step of placing a bet by the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for gambling. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of placing  
5 a bet by the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for gaming. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of playing a game by the  
10 individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for gaming. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism having a unique  
15 characteristic. Then there is the step of playing a game by the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for gaming. The method comprises the steps of recognizing a biometric signature  
20 of an individual having a sensor mechanism for sensing an acoustic characteristic. Then there is the step of playing a game by the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for gaming. The method comprises the steps of recognizing a biometric signature of an individual having a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of playing  
5 a game by the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing a utility box. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of  
10 allowing access to the utility box when the biometric signature of the individual is recognized.

Preferably, the allowing step includes the step of transmitting a usage reading of the utility when the biometric signature is recognized. The recognizing step preferably includes  
15 either the step of touching a touch mechanism of a recognizing mechanism to obtain the biometric signature of the individual, or placing a portion of the individual into a zone of a touchless mechanism of a recognizing mechanism to obtain the biometric signature of the individual.

20 Preferably, the touching step includes the step of touching electrodes of the touch mechanism for the recognizing mechanism to obtain the biometric signature of the individual or wherein the placing the portion step includes the step of placing the portion of the individual into an electric and/or magnetic

field in the zone to obtain the biometric signature of the individual. The touching step preferably includes the step of touching transducers of the touch mechanism for the recognizing mechanism to obtain the biometric signature of the individual, or  
5 wherein the placing the portion step includes the step of placing the portion of the individual in acoustic waves in the zone to obtain the biometric signature of the individual.

Preferably, the touching step includes the step of touching a card 170 with the electrodes for the individual to touch  
10 which provides the biometric signature of the individual. The touching step preferably includes the step of touching a card 170 with one or more transducers for the individual to touch which provides the biometric signature of the individual.

The present invention pertains to a method for accessing  
15 a utility box. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing access to the utility box when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for accessing a utility box. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an acoustic characteristic. Then there is the step of

allowing access to the utility box when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for accessing a utility box. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of allowing access to the utility box when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for accessing a meter. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of allowing access to the meter when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for accessing a meter. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing access to the meter when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for accessing a meter. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an acoustic characteristic. Then there is the step of allowing access



to the meter when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing a meter. The method comprises the steps of recognizing a biometric  
5 signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of allowing access to the meter when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for paying a fee. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of charging an account of the individual the fee when the biometric signature of the individual is recognized.

15 Preferably, the charging step includes the step of charging the account of the individual the fee over a telecommunication line in communication with a charging mechanism. The recognizing step preferably includes the step of placing a card  
170 having a memory 162 in communication with a card reader 174 of  
20 a cash register which reads the card 170 to obtain the biometric signature of the individual, and the charging step includes the step of charging the fee to the account of the individual with the cash register if the individual is recognized.

The present invention pertains to a method for paying a fee. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of charging an account of  
5 the individual the fee when the biometric signature of the individual is recognized.

The present invention pertains to a method for paying a fee. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism for sensing an  
10 acoustic characteristic. Then there is the step of charging an account of the individual the fee when the biometric signature of the individual is recognized.

The present invention pertains to a method for paying a fee. The method comprises the steps of recognizing a biometric  
15 signature of an individual with a sensor mechanism for sensing an electric and/or magnetic characteristic. Then there is the step of charging an account of the individual the fee when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing  
20 a vehicle or vehicular route. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of allowing access to the vehicle or vehicular route when the biometric signature of the individual is recognized.

Preferably, the allowing step includes the step of charging an account of the individual a fee to access the vehicle or vehicular route when a recognizing mechanism recognizes the individual. The charging step preferably includes the step of  
5 transmitting the fee and the biometric signature of the individual to a charging mechanism which recognizes the biometric signature of the individual and charges the fee to an account of the individual.

The present invention pertains to a method for accessing a vehicle or vehicular route. The method comprises the steps of  
10 recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing access to the vehicle or vehicular route when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing  
15 a vehicle or vehicular route. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of allowing access to the vehicle or vehicular route when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for accessing a vehicle or vehicular route. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then

there is the step of allowing access to the vehicle or vehicular route when the biometric signature of the individual is recognized.

The present invention pertains to a method for using a telecommunications apparatus for a communication. The method  
5 comprises the steps of recognizing a biometric signature of an individual. Then there is the step of allowing the communication with the telecommunications apparatus when the individual is recognized.

Preferably, the allowing step includes the step of  
10 charging an account of the individual a fee for the communication with the telecommunications apparatus when the individual is recognized.

Preferably, the charging step includes the step of  
15 charging the account over a telecommunications line. The telecommunications apparatus is preferably a telephone and wherein the allowing step includes the step of making a call on the telephone. Alternatively, the telecommunications apparatus is a video phone and wherein the allowing step includes the step of making a call on the video phone. Preferably, the recognizing step  
20 includes the step of recognizing the biometric signature of the individual with a sensor on a telephone.

The present invention pertains to a method for using a telecommunications apparatus for a communication. The method

comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing the communication with the telecommunications apparatus when the individual is recognized.

5           The present invention pertains to a method for using a telecommunications apparatus for a communication. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of allowing the  
10 communication with the telecommunications apparatus when the individual is recognized.

          The present invention pertains to a method for using a telecommunications apparatus for a communication. The method comprises the steps of recognizing a biometric signature of an  
15 individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of allowing the communication with the telecommunications apparatus when the individual is recognized.

          The present invention pertains to a method for watching  
20 a television. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of activating a television and/or channel of the television when the individual is recognized.

Preferably, the activating step includes the step of charging an account of the individual a fee for activating the television and/or channel when the individual is recognized. The charging step preferably includes the step of charging the account  
5 of the individual over a telecommunication line. Preferably, the activating step includes the steps of passing channels to the television through a mechanism for controlling passage of channels, and allowing the individual to activate predetermined channels of the television after the biometric signature of the individual is  
10 recognized. Preferably, the recognizing step includes the step of recognizing the biometric signature of the individual with a sensor on the television.

The present invention pertains to a method for watching a television. The method comprises the steps of recognizing a  
15 biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of activating a television and/or channel of the television when the individual is recognized.

The present invention pertains to a method for watching  
20 a television. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of activating a television and/or channel of the television when the individual is recognized.

The present invention pertains to a method for watching a television. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is  
5 the step of activating a television and/or channel of the television when the individual is recognized.

The present invention pertains to a method for checking out a book. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of  
10 checking out a book with a check-out box mechanism when the individual is recognized.

Preferably, the allowing step includes the step of charging an account of the individual the book when the individual is recognized.

15 The present invention pertains to a method for checking out a book. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of checking out a book with a check-out box mechanism when the individual is  
20 recognized.

The present invention pertains to a method for checking out a book. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism

sensing an acoustic characteristic. Then there is the step of checking out a book with a check-out box mechanism when the individual is recognized.

5 The present invention pertains to a method for checking out a book. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of checking out a book with a check-out box mechanism when the individual is recognized.

10 The present invention pertains to a method for boarding a plane. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of allowing the individual to pass through a gate to board the plane when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for boarding a plane. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing the individual to pass through a gate to board the plane when the biometric  
20 signature of the individual is recognized.

The present invention pertains to a method for boarding a plane. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an



acoustic characteristic. Then there is the step of allowing the individual to pass through a gate to board the plane when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for boarding a plane. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of allowing the individual to pass through a gate to board the plane when the biometric signature of the individual is recognized.

10 The present invention pertains to a method for passing through customs. The method comprises the steps of reading a known biometric signature of an individual from an electronic passport having a known biometric signature of the individual. Next there is the step of recognizing the biometric signature of the individual with a sensor mechanism having a unique characteristic. Then there is the step of allowing the individual through customs when the biometric signature of the individual is recognized from the known biometric signature of the individual.

20 The present invention pertains to a method for passing through customs. The method comprises the steps of reading a known biometric signature of an individual from an electronic passport having a known biometric signature of the individual. Next there is the step of recognizing the biometric signature of the individual with a sensor mechanism sensing an acoustic

characteristic. Then there is the step of allowing the individual through customs when the biometric signature of the individual is recognized from the known biometric signature of the individual.

5 The present invention pertains to a method for passing through customs. The method comprises the steps of reading a known biometric signature of an individual from an electronic passport having a known biometric signature of the individual. Next there is the step of recognizing the biometric signature of the individual with a sensor mechanism sensing an electric and/or  
10 magnetic characteristic. Then there is the step of allowing the individual through customs when the biometric signature of the individual is recognized from the known biometric signature of the individual.

15 Preferably, after the recognizing step there is the step of updating the passport when the individual passes through customs.

20 The present invention pertains to a method for applying a traffic citation or offense to an individual's license and record. The method comprises the steps of reading a known biometric signature of the individual from a driver's license having a known biometric signature of the individual. Next there is the step of recognizing a biometric signature of an individual. Then there is the step of recording the traffic citation or offense on the individual's license and record when the biometric signature

of the individual is recognized from the known biometric signature of the individual.

The present invention pertains to a method for applying a traffic citation or offense to an individual's license and record. The method comprises the steps of reading a known biometric signature of the individual from a driver's license having a known biometric signature of the individual. Next there is the step of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of recording the traffic citation or offense on the individual's license and record when the biometric signature of the individual is recognized from the known biometric signature of the individual.

The present invention pertains to a method for applying a traffic citation or offense to an individual's license and record. The method comprises the steps of reading a known biometric signature of the individual from a driver's license having a known biometric signature of the individual. Next there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of recording the traffic offense on the individual's license and record when the biometric signature of the individual is recognized from the known biometric signature of the individual.

The present invention pertains to a method for applying a traffic citation or offense to an individual's license and record. The method comprises the steps of reading a known biometric signature of the individual from a driver's license  
5 having a known biometric signature of the individual. Next there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of recording the traffic citation or offense on the individual's license and record when the  
10 biometric signature of the individual is recognized from the known biometric signature of the individual.

The present invention pertains to a method for accessing a room having computer terminals. The method comprises the steps of recognizing a biometric signature of an individual with a sensor  
15 mechanism having a unique characteristic. Then there is the step of unlocking a door to the room with the computer terminals when the individual is recognized.

The present invention pertains to a method for accessing a room having computer terminals. The method comprises the steps  
20 of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of unlocking a door to the room with the computer terminals when the individual is recognized.

The present invention pertains to a method for accessing a room having computer terminals. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then  
5 there is the step of unlocking a door to the room with the computer terminals when the individual is recognized.

The present invention pertains to a method for monitoring when an individual performs an action. The method comprises the steps of recognizing a biometric signature of an individual with a  
10 sensor mechanism having a unique characteristic. Then there is the step of a memory 162 having an account of the individual, the recognizing mechanism recording a time in an account of the individual when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for monitoring when an individual performs an action. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of a memory 162 having an account of the individual, the  
20 recognizing mechanism recording a time in an account of the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for monitoring when an individual performs an action. The method comprises the

steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of a memory 162 having an account of the individual, the recognizing mechanism recording a  
5 time in an account of the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing an account of an individual. The method comprises the steps of recognizing a biometric signature of an individual. Next there is  
10 the step of allowing access of the account of the when the biometric signature of the individual is recognized.

Preferably, the allowing step includes the step of allowing access of the account of the individual through a terminal when the biometric signature of the individual is recognized. The  
15 allowing step includes the step of allowing access to medical records of the individual in the account. Preferably, the allowing access step includes the step of accessing the account with a notepad. The allowing step includes the step of accessing a personal area network through which the biometric signature of the  
20 individual is provided and through which the account of the individual is accessed when the biometric signature of the individual is recognized.

Preferably, the allowing step includes the step of accessing the personal area network with a PAN wrist device

coordinating cellular phone, pager and personal digital assistant capabilities and which provides the biometric signature of the individual, when the biometric signature of the individual is recognized.

5           The present invention pertains to a method for accessing an account of an individual. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of allowing access of the account of the individual through a  
10 terminal when the biometric signature of the individual is recognized.

          The present invention pertains to a method for accessing an account of an individual. The method comprises the steps of recognizing a biometric signature of an individual with a sensor  
15 mechanism sensing an acoustic characteristic. Next there is the step of allowing access of the account of the individual through a terminal when the biometric signature of the individual is recognized.

          The present invention pertains to a method for accessing  
20 an account of an individual. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of allowing access of the account of the

individual through a terminal when the biometric signature of the individual is recognized.

The present invention pertains to a method for administering government benefits or funds. The method comprises  
5 the steps of recognizing a biometric signature of an individual. Next there is the step of lowering a value of benefits or funds in an account of the individual when the biometric signature of the individual is recognized.

Preferably, the lowering step includes the step of  
10 lowering food stamp value or Medicaid value in the account of the individual when the biometric signature of the individual is recognized. The lowering step includes the steps of touching by the individual sensors 333 of a card 170 having a microchip which contains data concerning the food stamp value and/or the Medicaid  
15 value and a known biometric signature of the individual, contacting a recognizing mechanism with the card 170 while the individual touches the sensors 333, recognizing with the recognizing mechanism the individual from the biometric signature of the individual obtained with the sensors 333 which is compared to the known  
20 biometric signature, and lowering the food stamp value or Medicaid value in the microchip.

The present invention pertains to a method for administering government benefits or funds. The method comprises the steps of recognizing a biometric signature of an individual



with a sensor mechanism having a unique characteristic. Next there is the step of lowering a value of benefits or funds in an account of the individual when the biometric signature of the individual is recognized.

5           The present invention pertains to a method for administering government benefits or funds. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of lowering a value of benefits or funds in an  
10 account of the individual when the biometric signature of the individual is recognized.

          The present invention pertains to a method for administering government benefits or funds. The method comprises the steps of recognizing a biometric signature of an individual  
15 with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of lowering a value of benefits or funds in an account of the individual when the biometric signature of the individual is recognized.

          The present invention pertains to a method for accessing  
20 an area. The method comprises the steps of touching by an individual a locking mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing a biometric signature of the individual. Next there is the step of opening the locking mechanism to access the area.

Preferably, the locking mechanism includes a handle of a door, and wherein the touching step includes the steps of touching by an individual a handle of a door to obtain the biometric signature of the individual. Then there is the step of opening  
5 step includes the step of opening the door with the handle. After the recognizing step there is preferably the step of recording in a memory 162 the identity of the individual and/or the time and date the individual touches the handle when the biometric signature of the individual is recognized.

10 Preferably, the recognizing step includes either the step of touching a touch mechanism of a recognizing mechanism on the handle to obtain the biometric signature of the individual, or placing a portion of the individual into a zone about the handle of a touchless mechanism of a recognizing mechanism to obtain the  
15 biometric signature of the individual. The touching step preferably includes the step of touching either electrodes or transducers of the touch mechanism for the recognizing mechanism to obtain the biometric signature of the individual, or wherein the placing the portion step includes the step of placing the portion  
20 of the individual into an electric and/or magnetic field in the zone or in acoustic waves in the zone to obtain the biometric signature of the individual. Preferably, the touching step includes the step of touching a card 170 with electrodes or transducers for the individual to touch which provides the biometric signature of  
25 the individual when the card 170 is in a card reader 174 to the card reader 174 adjacent, attached or integral to the door.

The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a locking mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing  
5 a biometric signature of the individual with a sensor mechanism having a unique characteristic. Then there is the step of opening the locking mechanism to access the area.

The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an  
10 individual a locking mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing a biometric signature of the individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of opening the locking mechanism to access the area.

15 The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a locking mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing  
20 a biometric signature of the individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of opening the locking mechanism to access the area.

Preferably, before the opening step there is the step of unlocking a lock of a door when the biometric signature of the

individual is recognized. Before the opening step, preferably there is the step of unlocking a lock of a door when the biometric signature of the individual is recognized. Preferably, before the opening step there is the step of unlocking a lock of a door when  
5 the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a handle having a sensor of an entry mechanism to the area to obtain the biometric signature of the individual. Next  
10 there is the step of recognizing a biometric signature of the individual. Next there is the step of opening the locking mechanism to access the area.

The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an  
15 individual a handle, having a sensor mechanism having a unique characteristic, of an entry mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing a biometric signature of the individual. Then there is the step of opening the locking mechanism to access the area.

20 The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a handle, having a sensor mechanism sensing an acoustic characteristic, of an entry mechanism to the area to obtain the biometric signature of the individual. Next there is the step of

recognizing a biometric signature of the individual. Then there is the step of opening the locking mechanism to access the area.

5 The present invention pertains to a method for accessing an area. The method comprises the steps of touching by an individual a handle, having a sensor mechanism sensing an electric and/or magnetic characteristic, of an entry mechanism to the area to obtain the biometric signature of the individual. Next there is the step of recognizing a biometric signature of the individual. Then there is the step of opening the locking mechanism to access  
10 the area.

15 The present invention pertains to a method for accessing data. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of accessing only authorized sections of a memory 162 or data storage mechanism by an individual when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for accessing data. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of accessing only authorized sections of a memory 162 or data storage mechanism by an individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing data. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of accessing only  
5 authorized sections of a memory 162 or data storage mechanism by an individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing data. The method comprises the steps of recognizing a biometric  
10 signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of accessing only authorized sections of a memory 162 or data storage mechanism by an individual when the biometric signature of the individual is recognized.

15 The present invention pertains to a method for accessing a network. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of accessing only authorized sections of the network with a network access mechanism when the biometric signature of the individual is  
20 recognized. Preferably, the network includes an Internet, an Extranet or an Intranet.

The present invention pertains to a method for accessing a network. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having

a unique characteristic. Next there is the step of accessing only authorized sections of the network with a network access mechanism when the biometric signature of the individual is recognized.

5 The present invention pertains to a method for accessing  
a network. The method comprises the steps of recognizing a  
biometric signature of an individual with a sensor mechanism  
sensing an acoustic characteristic. Next there is the step of  
accessing only authorized sections of the network with a network  
access mechanism when the biometric signature of the individual is  
10 recognized.

15 The present invention pertains to a method for accessing  
a network. The method comprises the steps of recognizing a  
biometric signature of an individual with a sensor mechanism  
sensing an electric and/or magnetic characteristic. Next there is  
the step of accessing only authorized sections of the network with  
a network access mechanism when the biometric signature of the  
individual is recognized.

20 The present invention pertains to a method for accessing  
software. The method comprises the steps of recognizing a  
biometric signature of an individual. Next there is the step of  
accessing the software when the biometric signature of the  
individual is recognized.

The present invention pertains to a method for accessing software. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of accessing the  
5 software when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing software. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism  
10 sensing an acoustic characteristic. Next there is the step of accessing the software when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing software. The method comprises the steps of recognizing a  
15 biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of accessing the software when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing  
20 computer 158. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of accessing the computer 158 when the biometric signature of the individual is recognized.



The present invention pertains to a method for accessing computer 158. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of accessing the  
5 computer 158 when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing computer 158. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism  
10 sensing an acoustic characteristic. Next there is the step of accessing the computer 158 when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing computer 158. The method comprises the steps of recognizing a  
15 biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of accessing the computer 158 when the biometric signature of the individual is recognized.

The present invention pertains to a method for  
20 protection. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of activating a weapon when the biometric signature of the individual is recognized, said recognizing mechanism integral to the weapon.

Preferably, the activating step includes the step of touching sensors 333 connected to an activating mechanism of the weapon to obtain the biometric signature of the individual, so the activating mechanism can be operated only when the biometric  
5 signature of the individual is recognized.

The present invention pertains to a method for protection. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of activating a  
10 weapon when the biometric signature of the individual is recognized, said recognizing mechanism integral to the weapon.

The present invention pertains to a method for protection. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism  
15 sensing an acoustic characteristic. Next there is the step of activating a weapon when the biometric signature of the individual is recognized, said recognizing mechanism integral to the weapon.

The present invention pertains to a method for protection. The method comprises the steps of recognizing a  
20 biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of activating a weapon when the biometric signature of the individual is recognized, said recognizing mechanism integral to the weapon.

The present invention pertains to a method for accessing drugs. The method comprises the steps of recognizing a biometric signature of an individual. Next there is the step of unlocking a lock of an area for holding drugs when the biometric signature of the individual is recognized so the individual can open the door to the area.

Preferably, the unlocking step includes the step of unlocking a lock of a door of a pharmacy cabinet, box or room for holding drugs when the biometric signature of the individual is recognized so the individual can open the door to the cabinet, box or room. After the unlocking step there is preferably the step of recording in a memory 162 the date, time and individual's identity each time the lock is unlocked.

Preferably, the unlocking step includes the steps of transmitting the biometric signature of the individual from a PAN card, receiving the transmitted biometric signature with a receiver connected to a recognizing mechanism connected to the lock, and unlocking the lock when the recognizing mechanism recognizes the biometric signature of the individual.

The present invention pertains to a method for accessing drugs. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of unlocking a lock of an area for holding drugs when the biometric signature of the

individual is recognized so the individual can open the door to the area.

The present invention pertains to a method for accessing drugs. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of unlocking a lock of an area for holding drugs when the biometric signature of the individual is recognized so the individual can open the door to the area.

The present invention pertains to a method for accessing drugs. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of unlocking a lock of an area for holding drugs when the biometric signature of the individual is recognized so the individual can open the door to the area.

The present invention pertains to a method for recognizing individual. The method comprises the steps of sensing with sensors 333 of a forehead mounted headset on an individual a biometric signature of an individual. Then there is the step of recognizing the individual from the biometric signature of the individual.

Preferably, after the sensing step there are the steps of transmitting the biometric signature of the individual with a transmitter on the headset. Then there is the step receiving the transmitted biometric signature of the individual at a recognizing mechanism. Next there is the step of the recognizing step includes the step of recognizing the biometric signature of the individual with the recognizing mechanism. Then after the recognizing step there are the steps of transmitting the electronic records in a memory 162 with a transmitter connected to the memory 162. Next there is the step of receiving with a receiver of the headset the transmitted electronic records. Then there is the step of viewing actual reality and the electronic records at the same time through glasses with a virtual screen having see through mode on the headset.

Before the viewing step there is preferably the step of examining an external working environment and wherein the viewing step includes the step of viewing the external working environment and the electronic records at the same time through glasses with the virtual screen having see through mode on the headset. Preferably, the electronic records include medical records and the external working environment includes a patient. The electronic records preferably include engineering schematics and the external working environment includes equipment. Preferably, the electronic records include maps.

The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors 333 of a forehead mounted headset on an individual a biometric signature of an individual. Then there is the step of  
5 recognizing the biometric signature of the individual with the recognizing mechanism with a sensor mechanism having a unique characteristic.

The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with  
10 sensors 333 of a forehead mounted headset on an individual a biometric signature of an individual. Then there is the step of recognizing the biometric signature of the individual with the recognizing mechanism with a sensor mechanism sensing an acoustic characteristic.

15 The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors 333 of a forehead mounted headset on an individual a biometric signature of an individual. Then there is the step of recognizing the biometric signature of the individual with the  
20 recognizing mechanism with a sensor mechanism sensing an electric and/or magnetic characteristic.

The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors 333 of a forehead mounted headset on an individual a

biometric signature of an individual. Next there is the step of transmitting the biometric signature of the individual with a transmitter on the headset. Next there is the step of receiving the transmitted biometric signature of the individual at a  
5 recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual with the recognizing mechanism communicating with the forehead sensor. Then there is the step of allowing access by the individual to the electronic records.

10 The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors 333 having a unique characteristic of a forehead mounted headset on an individual a biometric signature of an individual. Next there is the step of transmitting the biometric signature of  
15 the individual with a transmitter on the headset. Next there is the step of receiving the transmitted biometric signature of the individual at a recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual with the recognizing mechanism communicating with the forehead sensor with  
20 a sensor mechanism having a unique characteristic. Then there is the step of allowing access by the individual to the electronic records.

The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with  
25 sensors 333 sensing acoustic characteristics of a forehead mounted

headset on an individual a biometric signature of an individual. Next there is the step of transmitting the biometric signature of the individual with a transmitter on the headset. Next there is the step of receiving the transmitted biometric signature of the individual at a recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual with the recognizing mechanism communicating with the forehead sensor with a sensor mechanism sensing an acoustic characteristic. Then there is the step of allowing access by the individual to the electronic records.

The present invention pertains to a method for accessing electronic records. The method comprises the steps of sensing with sensors 333 for sensing electric and/or magnetic characteristics of a forehead mounted headset on an individual a biometric signature of an individual. Next there is the step of transmitting the biometric signature of the individual with a transmitter on the headset. Next there is the step of receiving the transmitted biometric signature of the individual at a recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual with the recognizing mechanism communicating with the forehead sensor with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of allowing access by the individual to the electronic records.

The present invention pertains to a method for accessing equipment. The method comprises the steps of recognizing a



biometric signature of an individual. Next there is the step of unlocking a lock to an area with the equipment disposed in it or to the equipment itself when the biometric signature of the individual is recognized so the individual can enter the area.

5            Preferably, the equipment includes a telecommunications switching system and wherein the unlocking step includes the step of unlocking a lock of a door of a cabinet with the telecommunications switching system disposed in it when the biometric signature of the individual is recognized so the  
10 individual can open the door to the cabinet.

            The present invention pertains to a method for accessing equipment. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is  
15 the step of unlocking a lock to an area with the equipment disposed in it or to the equipment when the biometric signature of the individual is recognized so the individual can enter the area.

            The present invention pertains to a method for accessing equipment. The method comprises the steps of recognizing a  
20 biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of unlocking a lock to an area with the equipment disposed in it or to the equipment itself when the biometric signature of the individual is recognized so the individual can enter the area.

The present invention pertains to a method for accessing equipment. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of  
5 unlocking a lock to an area with the equipment disposed in it or to the equipment itself when the biometric signature of the individual is recognized so the individual can enter the area.

The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric  
10 signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of unlocking a lock mechanism of an ATM machine which holds and dispenses cash when the biometric signature of the individual is recognized so the individual can access the ATM machine.

The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric  
15 signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of unlocking a lock mechanism of an ATM machine which holds and dispenses cash  
20 when the biometric signature of the individual is recognized so the individual can access the ATM machine.

The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an

electric and/or magnetic characteristic. Next there is the step of unlocking a lock mechanism of an ATM machine which holds and dispenses cash when the biometric signature of the individual is recognized so the individual can access the ATM machine.

- 5 Preferably, after the unlocking step there is the step of recording the date, time and individual's identity each time the ATM machine is unlocked.

The present invention pertains to a method for operating a vehicle or craft. The method comprises the steps of recognizing  
10 the biometric signature of the individual. Then there is the step of allowing the operation of the vehicle when the biometric signature of the individual is recognized.

- Preferably, before the recognizing step there is the step of touching a door handle of a door of the vehicle having sensors  
15 333 to obtain a biometric signature of an individual. The allowing step includes the step of unlocking a door lock of a vehicle when the biometric signature of the individual is recognized. Before the recognizing step there are the steps of touching a steering wheel of the vehicle having a sensor to obtain the biometric  
20 signature of the individual and starting an engine or motor of the vehicle when the biometric signature of the individual obtained from the sensors 333 is recognized. Preferably, before the recognizing step there are the steps of touching a sensor by the individual within reach of a seat for the individual to drive the  
25 vehicle to obtain the biometric signature of the individual, and

starting an engine or motor of the vehicle when the biometric signature of the individual obtained from the sensor is recognized.

5 The present invention pertains to a method for entering a vehicle or craft. The method comprises the steps of touching a door handle of a door of the vehicle having a sensor to obtain a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual with a sensor mechanism having a unique characteristic. Next there is the step of unlocking a door lock of a vehicle when the biometric signature  
10 of the individual is recognized.

15 The present invention pertains to a method for entering a vehicle or craft. The method comprises the steps of touching a door handle of a door of the vehicle having a sensor to obtain a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of unlocking a door lock of a vehicle when the biometric signature of the individual is recognized.

20 The present invention pertains to a method for entering a vehicle or craft. The method comprises the steps of touching a door handle of a door of the vehicle having a sensor to obtain a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next

there is the step of unlocking a door lock of a vehicle when the biometric signature of the individual is recognized.

The present invention pertains to a method for operating a vehicle. The method comprises the steps of inserting a key into  
5 a key entry of a vehicle. Then there is the step of recognizing a biometric signature of an individual. Next there is the step of engaging a motor or engine of the vehicle when the biometric signature of the individual is recognized and the key is inserted in the key entry.

10 Preferably, the recognizing step includes the step of touching a sensor integral to the key when the key is inserted into the key entry, and receiving current from the vehicle to obtain the biometric signature of the individual from the sensor integral to the key while the individual touches the sensor.

15 The present invention pertains to a method for operating a vehicle. The method comprises the steps of inserting a key into a key entry of a vehicle. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of  
20 engaging a motor or engine of the vehicle when the biometric signature of the individual is recognized and the key is inserted in the key entry.

The present invention pertains to a method for operating a vehicle. The method comprises the steps of inserting a key into

a key entry of a vehicle. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of engaging a motor or engine of the vehicle when the biometric  
5 signature of the individual is recognized and the key is inserted in the key entry.

The present invention pertains to a method for operating a vehicle. The method comprises the steps of inserting a key into a key entry of a vehicle. Then there is the step of recognizing a  
10 biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of engaging a motor or engine of the vehicle when the biometric signature of the individual is recognized and the key is inserted in the key entry.

The present invention pertains to a method for accessing an area. The method comprises the steps of inserting a key into a key entry of a lock to the area. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism in communication with the key. Next there is the step of  
15 opening the lock when the biometric signature of the individual is recognized and the key is inserted in the key entry.

The present invention pertains to a method for accessing an area. The method comprises the steps of inserting a key into a key entry of a lock to the area. Then there is the step of

recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic in communication with the key. Next there is the step of opening the lock when the biometric signature of the individual is recognized and the key is inserted  
5 in the key entry.

The present invention pertains to a method for accessing an area. The method comprises the steps of inserting a key into a key entry of a lock to the area. Then there is the step of recognizing a biometric signature of an individual with a sensor  
10 mechanism sensing an acoustic characteristic in communication with the key. Next there is the step of opening the lock when the biometric signature of the individual is recognized and the key is inserted in the key entry.

The present invention pertains to a method for accessing  
15 an area. The method comprises the steps of inserting a key into a key entry of a lock to the area. Then there is the step of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic in communication with the key. Next there is the step of opening  
20 the lock when the biometric signature of the individual is recognized and the key is inserted in the key entry.

The present invention pertains to a method for activating a control signal. The method comprises the steps of recognizing a biometric signature of an individual. Then there is the step of

producing a control signal with a transmitter for transmitting the control signal of a remote controller when the biometric signature of the individual is recognized.

Preferably, before the recognizing step there is the step  
5 of touching a sensor of the controller to obtain the biometric signature of the individual. The touching step preferably includes the step of touching the sensor on the controller to obtain the biometric signature of the individual. Preferably, before the recognizing step there is the step of placing a portion of the  
10 individual within a zone to obtain the biometric signature of the individual.

The present invention pertains to a method for activating a control signal. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique characteristic. Then there is the step of producing a  
15 control signal with a transmitter for transmitting the control signal of a remote controller when the biometric signature of the individual is recognized.

The present invention pertains to a method for activating  
20 a control signal. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Then there is the step of producing a control signal with a transmitter for transmitting the



control signal of a remote controller when the biometric signature of the individual is recognized.

The present invention pertains to a method for activating a control signal. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Then there is the step of producing a control signal with a transmitter for transmitting the control signal of a remote controller when the biometric signature of the individual is recognized.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signature of an individual from a transmitter of a touch mechanism of a wearing mechanism worn by an individual, said touch mechanism for obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Next there is the step of recognizing the biometric signature of the individual received at the receiver.

Preferably, the transmitting step includes the step of transmitting the biometric signal of the individual from a transmitter of a touch mechanism of an ankle band about an ankle of an individual or a touch mechanism of a wrist band about a wrist of the individual, said touch mechanism for obtaining the biometric signature of the individual. After the recognizing step there is

preferably the step of triggering an alarm if the biometric signature of the individual is not received at a predetermined time.

5 The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signal of an individual from a transmitter of a touch mechanism with a sensor mechanism having a unique characteristic of a wearing mechanism worn by an individual, said touch mechanism for obtaining the biometric signature of the individual. Next there is  
10 the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Next there is the step of recognizing the biometric signature of the individual received at the receiver.

15 The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signal of an individual from a transmitter of a touch mechanism with a sensor mechanism sensing an acoustic characteristic of a wearing mechanism worn by an individual, said touch mechanism for obtaining the biometric signature of the  
20 individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signal of an individual from a transmitter of a touch mechanism with a sensor mechanism sensing an electric and/or magnetic characteristic of a wearing mechanism worn by an individual, said touch mechanism for obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signature of an individual from a transmitter of a touch mechanism of a wearing mechanism worn by an individual, said touch mechanism for obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

Preferably, the transmitting step includes the step of transmitting the biometric signal of the individual from a transmitter of a touch mechanism of an ankle band about an ankle of an individual or a touch mechanism of a wrist band about a wrist of the individual, said touch mechanism for obtaining the biometric signature of the individual. After the recognizing step there is

the step of triggering an alarm if the biometric signature of the individual is not received at a predetermined time.

5 The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signal of an individual from a transmitter of a touch mechanism with a sensor mechanism having a unique characteristic of a wearing mechanism worn by an individual, said touch mechanism for obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

15 The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signal of an individual from a transmitter of a touch mechanism with a sensor mechanism sensing an acoustic characteristic of a wearing mechanism worn by an individual, said touch mechanism for obtaining the biometric signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a

biometric signal of an individual from a transmitter of a touch mechanism with a sensor mechanism sensing an electric and/or magnetic characteristic of a wearing mechanism worn by an individual, said touch mechanism for obtaining the biometric  
5 signature of the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for  
10 monitoring. The method comprises the steps of transmitting a biometric signature of an individual from a transmitter of a touchless mechanism, said touchless mechanism for obtaining the biometric signature of the individual remotely from the individual. Next there is the step of receiving the biometric signature with a  
15 receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a  
20 biometric signature of an individual from a transmitter of a touchless mechanism having a sensor mechanism with unique characteristics, said touchless mechanism for obtaining the biometric signature of the individual remotely from the individual. Next there is the step of receiving the biometric signature with a  
25 receiver at a location remote from the transmitter. Then there is

the step of recognizing the biometric signature of the individual received at the receiver.

5 The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signature of an individual from a transmitter of a touchless mechanism having a sensor mechanism sensing an acoustic characteristic, said touchless mechanism for obtaining the biometric signature of the individual remotely from the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

15 The present invention pertains to a method for monitoring. The method comprises the steps of transmitting a biometric signature of an individual from a transmitter of a touchless mechanism having a sensor mechanism sensing an electric and/or magnetic characteristic, said touchless mechanism for obtaining the biometric signature of the individual remotely from the individual. Next there is the step of receiving the biometric signature with a receiver at a location remote from the transmitter. Then there is the step of recognizing the biometric signature of the individual received at the receiver.

The present invention pertains to a method for monitoring. The method comprises the steps of obtaining a

biometric signature of an individual with a biometric mechanism worn by the individual. Next there is the step of transmitting a unique ID of the biometric mechanism and the biometric signal obtained from the biometric mechanism of the individual wearing the  
5 biometric mechanism with a transmitter/receiver of the biometric mechanism. Next there is the step of receiving the unique ID and the biometric signal at a recognizing mechanism with a transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of an individual  
10 with the recognizing mechanism. Then there is the step of determining where the individual is located.

Preferably, the biometric mechanism includes a touch mechanism which is touched by the individual to obtain the biometric signature of the individual. The biometric mechanism  
15 preferably includes a touchless mechanism having a zone in which a portion of the individual is placed to obtain the biometric signature of the individual.

The present invention pertains to a method for monitoring. The method comprises the steps of obtaining a  
20 biometric signature of an individual with a biometric mechanism with a sensor mechanism having a unique characteristic worn by the individual. Next there is the step of transmitting a unique ID of the biometric mechanism and the biometric signal obtained from the biometric mechanism of the individual wearing the biometric  
25 mechanism with a transmitter/receiver of the biometric mechanism.

Next there is the step of receiving the unique ID and the biometric signal at a recognizing mechanism with a transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of an individual with the recognizing  
5 mechanism. Then there is the step of determining where the individual is located.

The present invention pertains to a method for monitoring. The method comprises the steps of obtaining a biometric signature of an individual with a biometric mechanism  
10 worn with a sensor mechanism sensing an acoustic characteristic by the individual. Next there is the step of transmitting a unique ID of the biometric mechanism and the biometric signal obtained from the biometric mechanism of the individual wearing the biometric mechanism with a transmitter/receiver of the biometric mechanism.  
15 Next there is the step of receiving the unique ID and the biometric signal at a recognizing mechanism with a transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of an individual with the recognizing mechanism. Then there is the step of determining where the  
20 individual is located.

The present invention pertains to a method for monitoring. The method comprises the steps of obtaining a biometric signature of an individual with a biometric mechanism worn with a sensor mechanism sensing an electric and/or magnetic  
25 characteristic by the individual. Next there is the step of



transmitting a unique ID of the biometric mechanism and the biometric signal obtained from the biometric mechanism of the individual wearing the biometric mechanism with a transmitter/receiver of the biometric mechanism. Next there is the  
5 step of receiving the unique ID and the biometric signal at a recognizing mechanism with a transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of an individual with the recognizing mechanism. Then there is the step of determining where the  
10 individual is located.

The present invention pertains to a method for tracking. The method comprises the steps of obtaining a biometric signature of an individual. Next there is the step of sending information and the biometric signature of the individual with an individual  
15 transmitter/receiver to a recognizing transmitter/receiver of a recognizing mechanism for recognizing the individual. Next there is the step of receiving the information and the biometric signature of the individual with the transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the  
20 biometric signature of the individual. Next there is the step of ascertaining the position of the individual from a GPS.

Preferably, the sending step includes the step on inserting a controller PAN touch sensor card 170 for obtaining the biometric signature of the individual into the individual  
25 transmitter/receiver.

The present invention pertains to a method for tracking. The method comprises the steps of obtaining a biometric signature of an individual with a sensor mechanism having a unique characteristic. Next there is the step of sending information and  
5 the biometric signature of the individual with an individual transmitter/receiver to a recognizing transmitter/receiver of a recognizing mechanism for recognizing the individual. Next there is the step of receiving the information and the biometric signature of the individual with the transmitter/receiver of the  
10 recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual. Next there is the step of ascertaining the position of the individual from a GPS.

The present invention pertains to a method for tracking. The method comprises the steps of obtaining a biometric signature of an individual with a sensor mechanism sensing an acoustic  
15 characteristic. Next there is the step of sending information and the biometric signature of the individual with an individual transmitter/receiver to a recognizing transmitter/receiver of a recognizing mechanism for recognizing the individual. Next there  
20 is the step of receiving the information and the biometric signature of the individual with the transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the biometric signature of the individual. Next there is the step of ascertaining the position of the individual from a GPS.

The present invention pertains to a method for tracking. The method comprises the steps of obtaining a biometric signature of an individual. Next there is the step of sending information and the biometric signature of the individual with an individual  
5 transmitter/receiver to a recognizing transmitter/receiver of a recognizing mechanism for recognizing the individual. Next there is the step of receiving the information and the biometric signature of the individual with the transmitter/receiver of the recognizing mechanism. Next there is the step of recognizing the  
10 biometric signature of the individual with a sensor mechanism sensing an electric and/or magnetic characteristic. Next there is the step of ascertaining the position of the individual from a GPS.

The present invention pertains to a method for tracking. The method comprises the steps of recognizing the biometric  
15 signature of the individual. Next there is the step of ascertaining the position of the individual from a GPS when the biometric signature of the individual is recognized.

The present invention pertains to a method for tracking. The method comprises the steps of recognizing the biometric  
20 signature of the individual with a sensor mechanism having a unique characteristic. Next there is the step of ascertaining the position of the individual from a GPS when the biometric signature of the individual is recognized.

The present invention pertains to a method for tracking. The method comprises the steps of recognizing the biometric signature of the individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of ascertaining  
5 the position of the individual from a GPS when the biometric signature of the individual is recognized.

The present invention pertains to a method for tracking. The method comprises the steps of recognizing the biometric signature of the individual with a sensor mechanism sensing an  
10 electric and/or magnetic characteristic. Next there is the step of ascertaining the position of the individual from a GPS when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric  
15 signature of an individual. Next there is the step of identifying an amount of cash to be distributed to the individual in a control unit. Then there is the step of distributing cash to the individual when the biometric signature of the individual is recognized.

20 Preferably, the identifying step includes the step of identifying the amount of cash to be distributed to the individual in an ATM machine, and the distributing step includes the step of distributing cash to the individual from the ATM machine when the biometric signature of the individual is recognized. Before the

distributing step there is preferably the step of charging an account of the individual by the control unit the amount of cash to be distributed to the individual, and the distributing step includes the step of distributing cash to the individual from the  
5 control unit when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism having a unique  
10 characteristic. Next there is the step of identifying an amount of cash to be distributed to the individual in a control unit. Then there is the step of distributing cash to the individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing  
15 cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an acoustic characteristic. Next there is the step of identifying an amount of cash to be distributed to the individual in a control unit. Then there is the step of distributing cash to the  
20 individual when the biometric signature of the individual is recognized.

The present invention pertains to a method for accessing cash. The method comprises the steps of recognizing a biometric signature of an individual with a sensor mechanism sensing an

electric and/or magnetic characteristic. Next there is the step of identifying an amount of cash to be distributed to the individual in a control unit. Then there is the step of distributing cash to the individual when the biometric signature of the individual is  
5 recognized.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism by the individual to generate a biometric signature of the individual. Next there is the step of  
10 placing the sensor mechanism in communication with a reader 174. Then there is the step of reading the sensor mechanism with the reader 174 and recognizing the individual from the biometric signature.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism with a unique characteristic by the individual to generate a biometric signature of the individual. Next there is the step of placing the sensor mechanism in communication with a reader 174. Then there is the step of reading  
15 the sensor mechanism with the reader 174 and recognizing the individual from the biometric signature.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism for sensing an acoustic characteristic

by the individual to generate a biometric signature of the individual. Next there is the step of placing the sensor mechanism in communication with a reader 174. Then there is the step of reading the sensor mechanism with the reader 174 and recognizing  
5 the individual from the biometric signature.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism for sensing an electric and/or magnetic characteristic by the individual to generate a biometric signature  
10 of the individual. Next there is the step of placing the sensor mechanism in communication with a reader 174. Then there is the step of reading the sensor mechanism with the reader 174 and recognizing the individual from the biometric signature.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism by the individual to generate a biometric signature of the individual. Then there is the step of reading the sensor mechanism to obtain the biometric signature of the individual and a memory 162 having known biometric signatures  
15 with a reader 174. Then there is the step of recognizing the individual from the biometric signature.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism with a unique characteristic by the

individual to generate a biometric signature of the individual. Then there is the step of reading the sensor mechanism to obtain the biometric signature of the individual and a memory 162 having known biometric signatures with a reader 174. Then there is the  
5 step of recognizing the individual from the biometric signature.

The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism for sensing an acoustic characteristic by the individual to generate a biometric signature of the  
10 individual. Then there is the step of reading the sensor mechanism to obtain the biometric signature of the individual and a memory 162 having known biometric signatures with a reader 174. Then there is the step of recognizing the individual from the biometric signature.

15 The present invention pertains to a method for authenticating an individual. The method comprises the steps of touching a sensor mechanism for sensing an electric and/or magnetic characteristic by the individual to generate a biometric signature of the individual. Then there is the step of reading the sensor  
20 mechanism to obtain the biometric signature of the individual and a memory 162 having known biometric signatures with a reader 174. Then there is the step of recognizing the individual from the biometric signature.



The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of the individual with a touchless sensor for a non-facial feature of the individual. Then  
5 there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of the individual with a touchless sensor having a unique characteristic for a non-facial  
10 feature of the individual. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of the individual with a touchless sensor for sensing an acoustic characteristic for a non-facial  
15 feature of the individual. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of the individual with a touchless sensor for sensing an electric and/or magnetic  
20 characteristic for a non-facial feature of the individual. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of flipping up a flip-up sensor for obtaining a biometric signature of an individual. Next there is the step of touching by the individual  
5 the sensor. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of flipping  
10 up a flip-up sensor having a unique characteristic for obtaining a biometric signature of an individual. Next there is the step of touching by the individual the sensor. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to  
15 occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of flipping up a flip-up sensor for sensing an acoustic characteristic for obtaining a biometric signature of an individual. Next there is  
20 the step of touching by the individual the sensor. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of flipping up a flip-up sensor for sensing an electric and/or magnetic characteristic for obtaining a biometric signature of an individual. Next there is the step of touching by the individual the sensor. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of touching by the individual a recessed sensor for obtaining a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of touching by the individual a recessed sensor having a unique characteristic for obtaining a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of touching by the individual a recessed sensor for sensing an acoustic

characteristic for obtaining a biometric signature of an individual. Next there is the step of recognizing the biometric signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

5           The present invention pertains to a method for authorizing an action. The method comprises the steps of touching by the individual a recessed sensor for sensing an electric and/or magnetic characteristic for obtaining a biometric signature of an individual. Next there is the step of recognizing the biometric  
10 signature of the individual obtained with the sensor. Then there is the step of allowing the action to occur.

          The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of an individual with a biometric  
15 PAN system having a sensor for obtaining the biometric signature of the individual. Then there is the step of allowing the action to occur.

          The present invention pertains to a method for authorizing an action. The method comprises the steps of  
20 recognizing a biometric signature of an individual with a biometric PAN system having a sensor with a unique characteristic for obtaining the biometric signature of the individual. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of an individual with a biometric PAN system having a sensor for sensing an acoustic characteristic  
5 for obtaining the biometric signature of the individual. Then there is the step of allowing the action to occur.

The present invention pertains to a method for authorizing an action. The method comprises the steps of recognizing a biometric signature of an individual with a  
10 biometric PAN system having a sensor for sensing an electric and/or magnetic characteristic for obtaining the biometric signature of the individual. Then there is the step of allowing the action to occur.

The present invention pertains to a method for  
15 authorizing an action. The method comprises the steps of detecting a characteristic of an individual from energy emitted by the individual. Then there is the step of recognizing a biometric signature of the individual from the energy. Next there is the step of allowing the action to occur.

20 The present invention pertains to an apparatus for authorizing an action, as shown in figure 200. The apparatus comprises a mechanism for recognizing a biometric signature of an individual from energy emitted by the individual. The apparatus comprises a mechanism for allowing the action when the recognizing

mechanism recognizes the biometric signature of the individual. The allowing mechanism is connected to the recognizing mechanism.

Living, metabolizing organisms manipulate energy in many different forms, including acoustic, magnetic, electric, and  
5 electromagnetic. Living organisms produce energy which can be detected. The energy pattern which a specific organism produces is unique for that organism.

The energy pattern of an organism can be detected actively or passively. In Fig. 11, the energy pattern of the  
10 organism is detected by looking at how the organism's energy pattern interacts with the energy provided. By applying a known energy pattern, and examining how the known energy pattern is changed by the organism, the organism's inherent energy pattern is detected. In a passive system, as shown in figure 200 and 207, the  
15 organism's inherent energy pattern is detected, without applying an outside energy field. Regardless of whether the electric and/or magnetic properties actively or passively is detected, the same properties are still being detected.

For an example of a passive detection system, a  
20 stationary, pressure activated, curved detector band is used, against which the individual presses their forehead. The detector band is fitted with E-field probes with pseudo vector information. See "E-Field Probe With Pseudo-Vector Information" by K. Pokovic. T. Schmid, J. Frohlich, N. Chavannes and N. Kuster; Swiss Federal

Institute of Technology (ETH), CH-8092, Zurich, Switzerland, incorporated by reference herein. This probe type allows precise measurement of electric field strength distributions in complex environments, giving information about the field amplitude as well  
5 as the field polarization at any measured location. By putting several probes in the detector band, a measurement can be taken at several locations.

When the individual presses their forehead against the detector band, they say their name out loud. The  
10 electroencephalographic pattern produced when a person pronounces their own name will be unique based on the electrical patterns produced in multiple areas of the brain such as the motor areas, sensory areas, speech centers, and emotional centers. This will produce a unique pattern of electric field amplitudes and  
15 polarizations at the detector band.

The electrical activity of the brain is usually divided into three categories: 1) spontaneous potentials such as alpha and beta rhythms, 2) evoked or event related potentials, and 3) single neuron potential recorded with microelectrodes. Electric Fields of  
20 the Brain: The Neurophysics of EEF. P.L. Nunez and R.D. Katznelson, Oxford Univ. Press, 1981; incorporated by reference herein. The primary structures of the brain are the brainstem, midbrain (thalamus), cerebellum, and cerebrum (including cerebral cortex). The cortex is vital to much of our conscious experience.

It is believed to produce most of the electrical potentials measured on the scalp.

Traditionally, scalp (cortex) potentials are described by their amplitude, frequency, and spatial characteristics. Electric  
5 Fields of the Brain: The Neurophysics of EEG. P.L. Nunez and R.D. Katznelson, Oxford Univ. Press, 1981; incorporated by reference herein. The unique characteristics of scalp potentials from any particular individual depend on the nature, location, and patterns in the electrical current sources in the cortex. The unique  
10 characteristics from an individual also depend on the electrical and structural geometric properties of the individual's brain, skull, and scalp as well.

In the embodiment described above, the spontaneous and event related potentials produced by the cortex is measured, and  
15 transmitted through the geometric structures of the brain (two hemispheres), skull, and scalp. The background spontaneous potential will tend to vary for an individual from day to day, depending on their mood and state of health, however, the spontaneous potential produced by a person truthfully stating their  
20 own name will be a significant EEG marker. If the same person pronounces two different words, the event potentials will be different because the muscle sequences required to say the two names will be different. Thus, an individual will have one event potential when the individual says one name, and a different one  
25 when the individual says a second name. The combined spontaneous



and event related potentials will thus be unique for an individual truthfully stating their own name.

Now what if two people have the same name? Their combined spontaneous and event related potentials will still be different  
5 because no two people have the identical set of memories and neuromotor connections. Also, since the cortex produced electric field must be transmitted through their differing brains, skulls, and scalps, even if their spontaneous and event related potentials were identical, the field detected at the scalp (forehead) would be  
10 different and unique.

Scalp measurements vary depending on the strength of the electric field and distance between it and the sensors. They range from about 0.1 to 200  $\mu V$  at the scalp and are around 500  $\mu V$  in the cortex itself. Various probe and data processing techniques can  
15 also be used such as bipolar recordings, average reference recording, linked-ears reference, spectral analysis, Laplace derivations, frequency-wavenumber spectra, orthogonal and/or Bessel functions in temporal and/or spatial domains, Fourier transforms, and multichannel preprocessing by matrix operations.

20 The above embodiment could be combined with an active electric/magnetic or acoustic forehead sensor system, or with a voice recognition system. It can also be incorporated into a portable forehead mounted system such as we have already described for the active systems.

In regard to another embodiment of the hand unit, otherwise referred to as the Hand Pad Biometric Impedance System (HBIS), the following description is provided.

#### Elements of the HBIS

5

1. Dolch Computer, Inc. portable computer, the FieldPAC.
2. National Instruments Data Acquisition Board (DAQ board model PCI-MIN-16E-1)
3. Hand Pad Electronics Box

10

- a. Connection to DAQ board through shielded cable
- b. Six electrodes built into top of box for placement of hand
- c. External connector with pins that connect directly to the electrodes through extension wires
- d. Active circuitry for ensuring constant current through a variable load over a wide range of frequencies

15

4. Software

20

1. LabVIEW runtime engine for executing LabVIEW graphical code, version 5.1.
2. *Biometric Recognition*, source code that interfaces with the user and controls the Hand Pad box (via the DAQ board) so as to automatically conduct impedance measurements of the hand according to user specifications (3 and 5 finger versions)

3. NI-DAQ driver software to interface between the DAQ board and the LabVIEW executable
4. Configuration software to control DAQ board settings and associate it with a device number

## 5 Active circuitry for ensuring constant current in a variable load

With reference to figure 199, active circuitry means use of an operational amplifier (OA). Constant current is achieved when OA is used in a negative feedback arrangement. The current path is from the analog output (AO) through the input resistor R1, and through the feedback impedance R2 or some finger of the hand, and to the output terminal of the OA (returning to the DAQ board via the signal ground (SG) via the +-15V power connections to the OA). No significant current enters the (+) or (-) terminals of the OA because they are high impedance.

Negative feedback means that the input terminals have equal voltage. Since the (+) terminal is fixed to ground (SG) then the (-) terminal must also be 0 volts all the time. Hence the current in the circuit is uniquely determined by the voltage of AO ( $V_{AO}$ ) divided by R1 (Ohm's Law).  $I = V_{AO}/R1$ . Since this current does not split, it must travel through the hand regardless of its impedance. Hence the voltage at the palm (= output voltage of OA and = to voltage across hand) is determined (Ohm's Law):  $V_{palm} = I * Z_{hand}$ . The equation for  $Z_{hand}$  needs only  $V_{AO}$  which is set by the

software,  $V_{palm}$  which is measured at channel 6 of the analog input, and R1 which is fixed and known.

#### Other elements of the electronics

5 +5V power is sensed at AI channel 1 to be certain that there is a good connection between the computer and the hand pad box. +5V power is sensed at AI channel 0 to be certain that the fuse is intact. Fused +5V power is used to provide power to the OA via a dc to dc converter and to drive all relay switches. The connector board on which the circuit was built originally came with  
10 a 0.8 amp 5mm x 20mm fuse. I have used 0.5 amp and 1.0 amp fuses. Do not use greater than 1 amp fuses as damage to the DAQ board may result.

Digital output (DO, +5V - high, 0V = low) lines control transistors (Q) that turn on or off relay switches. Transistors are  
15 switches themselves but are not suitable for bipolar signals such as ac sinewaves. Relay switches are used to send current through one finger at a time.

An additional switch is used to put the active circuit in a constant voltage mode. This feature has been disabled in  
20 Biometric Recognition because constant voltage mode is unreliable compared to constant current mode. However, this feature is still available in the test program. One digital line controls a pair of relay switches that reverse the position of R1 and the hand

impedance. R1 becomes the feedback resistor and a current sensing resistor. The voltage across the hand is constant if AO is constant (meaning the peak voltage).

When data is not actively being taken another switch sets  
5 R2 as the feedback resistor. If there is no feedback resistance, then the output of OA will saturate, i.e. it will go to the maximum magnitude voltage (+ or - 15 volts) in an attempt to control the voltage at the (-) input terminal and make it 0V. Once finite feedback resistance is restored after the OA has saturated, it  
10 takes time (longer than relay switching time) for it to recover to a stable operating mode. In this case double Zener (Z) diodes at the OA output clamp the voltage to between + and - 10.2 volts to protect the inputs on the DAQ board.

The driving AO voltage is sampled at AI channel 7. The AO  
15 voltage is reliable and need not be double checked, but AI chan 7 is sampled in differential mode, i.e., with respect to the virtual ground at the (-) terminal, not the signal ground (SG). Therefore any significant difference between AO and AI7 mean that there is no virtual ground and the OA is not operating in stable mode. Data  
20 measurements are thus disregarded.

Stray capacitance is a nuisance. It provides a point for the current to split and bypass the rest of the circuit, especially at high frequencies. Capacitive impedance in parallel with  $Z_{hand}$

allows a smaller effective feedback impedance. Hence, even fixed resistors appear to lose resistance as the frequency increases.

Another issue is phasing. AO drives a sinewave that attempts to put a sinewave voltage on the (-) terminal. The OA  
5 output responds by driving a negative sinewave (alternatively, a wave  $180^\circ$  out of phase) that cancels the response at (-) terminal thereby making it a constant 0V. When there is capacitance in the feedback, the  $180^\circ$  phasing is upset and a small sinewave ripple appears on the virtual ground. It grows at higher frequencies and  
10 no longer operates in a stable feedback mode.

Part of the source of this parallel capacitance is the pair of wires leading to AI chan 6 and AI chan 14. Placing shielding around the wires in the electronics box alleviates the problem by diverting the capacitance from across the hand to  
15 ground. This simply becomes a demand for more current from OA, which can supply up to 30 mA compared to the 10s of  $\mu\text{A}$  in the feedback circuit (which is limited by R1). Similarly, pairs of wires leading to the external connector (and to an external hand pad if one should be connected) introduce stray capacitance. These  
20 too have also been shielded. Nevertheless, there is still the characteristic roll off in fixed resistive impedance versus frequency. As long as the intrinsic capacitance of the hand is less than the stray capacitance, the stray capacitance should not be an influence.

5 are collected. The AI waveform is Fourier analyzed to determine the amplitude at the measurement frequency.

10 voltage that can be sampled at the AI input. The AO amplitude must  
be chosen to maximize the AI amplitude in order to defeat the noise  
that hampers precise reproducibility needed for identification and  
verification functions.

15 what is meant by "constant current". Originally it meant the same  
current for all frequencies, fingers, and impedances. This meant  
that the AO signal had to be tiny in order to measure the highest  
impedances (so as not to exceed the AI limit), but then the AI  
signal was too small for all other measurements. Then the AO  
20 amplitude was a function of the frequency assuming that the hand  
impedance decreased as the frequency increased.

Constant current is taken to mean only that the current is constant in each of the fingers of the hand for a single frequency measurement of the hand. The hand impedance is regarded

as only one measurement and individual finger impedances are only elements of the measurement. The current in the hand then may be different for two people measuring at the same frequency. It may be different for the same person measuring at the same frequency on  
5 different occasions, although this difference is expected to be slight.

The method to choose the AO amplitude is based on maximizing the AI signal. The fingers are crudely measured with only one  $\mu$ amp of current. The finger with the highest impedance is  
10 used to determine AO so that the AI amplitude is 9.5 V (near maximum but not quite). AO is fixed and the current is constant and the measurement proceeds more carefully. For each finger as many 4 cycle measurements are taken as possible in the allotted dwell time. The mean of these measurements is the finger impedance and  
15 their standard deviation is the statistical error. For impedances greater than R1, AO is less than 9.5 V.

For impedances less than R1 then AO = 9.5 V and the current is constant all the time, all frequencies, all hands. In this case AI is always less than 9.5 V and as much signal as  
20 possible that can be obtained is measured. It makes sense to make R1 as small as possible, but on the other hand AO must be made tiny to measure large impedances and the quality of sinewave synthesis begins to suffer. The  $\Delta V$  between digital points is 2.5 mV. The result is that R1 should be between 10 k $\Omega$  and 200 k $\Omega$ .



The present invention pertains to an apparatus for accessing an area. The apparatus comprises a mechanism 293 for determining a biometric signature of an individual, as shown in figure 201. The apparatus comprises a door having a door handle in which electrodes 333 are disposed to obtain the biometric signature of the individual when the individual grabs or touches the handle, and a lock. The apparatus comprises a reader 174 for reading the biometric signature of the individual from the electrodes 333. The reader 174 is connected to the determining mechanism 293 and the electrodes 333. The apparatus comprises a memory 162 having a known biometric signature of the individual. The determining mechanism 293 is connected to the memory 162 and compares the known biometric signature of the individual with the biometric signature of the individual obtained from the electrodes 333. The apparatus comprises a mechanism 335 for unlocking the lock when the determining mechanism 293 recognizes the biometric signature of the individual from the known biometric signature of the individual. The unlocking mechanism 335 is connected to the determining mechanism 293.

The apparatus includes a numerical keypad in which an entry code is entered, as shown in figure 202. The keypad 397 is connected to the determining mechanism 293. The memory 162 has a predetermined entry code associated with the individual. The unlocking mechanism 335 unlocks the lock when the determining mechanism 293 recognizes the biometric signature of the individual from the known biometric signature of the individual and receives

a predetermined entry code associated with the individual from the keypad 397.

The door handle preferably has a thumb flap having an acoustic transducer 333 for obtaining with the electrodes 333, the biometric signature of the individual, as shown in figure 203. Preferably, the lock has a key slot, and includes a key, as shown in figure 206, and can or cannot include the acoustic transducer. The unlocking mechanism 335 unlocking the lock when the determining mechanism 293 recognizes the biometric signature of the individual from the known biometric signature of the individual and the key is in the key slot. The transducer 333 preferably obtains a thumb biometric signature of the individual, and includes a thumb flap reader 174 connected to the transducer in the thumb flap, and a thumb flap memory 162 having a known biometric thumb signature connected to the determining mechanism 293, as shown in figure 205. The determining mechanism 293 compares the thumb biometric signature with the known thumb biometric signature. The unlocking mechanism 335 unlocking the lock when the determining mechanism 293 recognizes the biometric signature of the individual from the known biometric signature of the individual and the thumb biometric signature from the known thumb biometric signature.

Preferably, the determining mechanism 293 includes an electrode determining mechanism 293 connected to the memory 162 and the reader 174 for comparing the known biometric signature of the individual with the biometric signature of the individual obtained

from the sensors 333, a thumb flap determining mechanism 293 connected to the thumb flap memory 162 and the thumb flap reader 174 for comparing the known thumb biometric signature with the biometric signature obtained from the transducer and the thumb flap, and including a key slot connected to the electrode determining mechanism 293 and the thumb flap determining mechanism 293, and a key for insertion into the key slot. See figure 204. The unlocking mechanism allowing unlocking the lock when the electrode determining mechanism 293 recognizes the biometric signature of the individual from the known biometric signature of the individual, the thumb flap determining mechanism 293 recognizes the thumb biometric signature of the individual from the known thumb biometric signature of the individual, and the key can be placed in the key slot to unlock the lock.

The present invention pertains to a method for accessing an area. The method comprises the steps of grabbing or touching by an individual a door handle of a door in which sensors 333 are disposed to obtain the biometric signature of the individual. Then there is the step of reading the biometric signature of the individual from the sensors. Next there is the step of comparing a known biometric signature of the individual with the biometric signature of the individual obtained from the sensors. Then there is the step of unlocking a lock of the door when the biometric signature of the individual from the known biometric signature of the individual is recognized.

Preferably, the unlocking step includes the steps of entering an entry code into a numerical keypad, and unlocking the lock when the biometric signature of the individual is recognized from the known biometric signature of the individual and a  
5 predetermined entry code associated with the individual is entered into the keypad. The unlocking step preferably includes the step of touching an acoustic transducer of a thumb flap of the door handle. In other embodiment, other mechanisms for entering a predetermined entry code may be used such as bar codes, magnetic  
10 strips, etc.

Preferably, the step of unlocking includes the steps of inserting a key into a key slot of a lock, and unlocking the lock when the biometric signature of the individual is recognized from the known biometric signature of the individual and the key is in  
15 the key slot. The unlocking step preferably includes the steps of obtaining a thumb biometric signature of the individual, comparing the thumb biometric signature with the known thumb biometric signature, and unlocking the lock when the biometric signature of the individual is recognized from the known biometric signature of  
20 the individual and the thumb biometric signature is recognized from the known thumb biometric signature. Preferably, the unlocking step includes the steps of obtaining a thumb biometric signature of the individual by touching an acoustic transducer of a thumb flap of the door handle, comparing the thumb biometric signature with  
25 the known thumb biometric signature, and unlocking the lock when the biometric signature of the individual is recognized from the

known biometric signature of the individual and the thumb biometric signature is recognized from the known thumb biometric signature and the key is in the key slot.

5 The present invention pertains to a method and apparatus for an operational biometric device, wherein the method of authorizing an action or recognizing an individual is performed as part of the customary operation of a device.

10 Although the invention has been described in detail in the foregoing embodiments for the purpose of illustration, it is to be understood that such detail is solely for that purpose and that variations can be made therein by those skilled in the art without departing from the spirit and scope of the invention except as it may be described by the following claims.